# Arrêté du 18 août 2016 portant approbation de la politique ministérielle de défense et de sécurité

**NOR : JUST1624217A**

Le garde des sceaux, ministre de la justice,

*Vu le code de la défense, notamment ses articles L.1332-1 à L.1332-7 et R.1332-1 à R.1332-42 ;*
*Vu le décret du 25 juillet 2005 relatif aux délégations de signature des membres du gouvernement ;*
*Vu le décret du 26 septembre 2013 portant nomination du secrétaire général du ministère de la justice ;*
*Vu le décret du 23 octobre 2013 portant nomination du haut fonctionnaire de défense et de sécurité du ministère de la justice ;*
*Vu l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activité d'importance vitale et désignant les ministres coordonnateurs desdits secteurs ;*
*Vu l'arrêté du 20 avril 2009 portant désignation des opérateurs d'importance vitale relevant du secteur d'activité d'importance vitale des activités judiciaires ;*
*Vu l'arrêté du 13 septembre 2013 portant approbation de la politique ministérielle de défense et de sécurité ;*
*Vu l'arrêté du 23 mai 2016 portant approbation de la directive nationale de sécurité des activités judiciaires ;*
*Sur proposition du secrétaire général,*

ARRÊTE

**Article 1**

La politique ministérielle de défense et de sécurité, ci-après annexée, est approuvée.

**Article 2**

L'arrêté n° 13–015 du 13 septembre 2013 portant approbation de la politique ministérielle de défense et de sécurité est abrogé.

**Article 3**

Le présent arrêté sera publié au Bulletin officiel du ministère de la justice.

Fait à Paris le 18 août 2016.

Pour le garde des sceaux et par délégation,
Le secrétaire général,

**Éric LUCAS**


**Secrétariat général**
**Haut fonctionnaire de défense et de sécurité**

# SAIVAJ

## SECTEUR D'ACTIVITÉS D'IMPORTANCE VITALE DES ACTIVITÉS JUDICIAIRES

**---oooOooo---**

**Directive nationalede sécuritédes activités judiciaires**

**---oooOooo---**

# PMDS

# Politique ministérielle de défense et de sécurité

| CIRCUIT DE VALIDATION | | | | | |
|---|---|---|---|---|---|
| **DATE** | **Rev.** | **OBJET** | **Rédaction** | **Vérif.** | **Approbation** |
| 02/01/2008 | 1 | Directive nationale de sécurité des activités judiciaires | Gerald Bartholomew<br>David Crochemore | GB-DC | Marc Moinard<br>Premier ministre |
| 01/09/2008 | 2 | Politique ministérielle de défense et de sécurité | Gerald Bartholomew<br>David Crochemore | GB-DC | Gilbert Azibert |
| 14/08/2010 | 3 | Politique ministérielle de défense et de sécurité ; Modifications diverses | Gerald Bartholomew<br>David Crochemore | GB-DC | Emmanuel Rébeillé-Borgella |
| 04/11/2010 | 4 | Politique ministérielle de défense et de sécurité ;<br>Amendements Conseil d'Etat | Gerald Bartholomew<br>David Crochemore | GB-DC | Emmanuel Rébeillé-Borgella |
| 13/01/2011 | 5 | Politique ministérielle de défense et de sécurité ; Modifications diverses | Gerald Bartholomew<br>David Crochemore | GB-DC | Emmanuel Rébeillé-Borgella |
| 11/01/2013 | 6 | Politique ministérielle de défense et de sécurité ; Révision générale | Gerald Bartholomew<br>Luc Vallée | GB-LV | André Gariazzo |
| 13/09/2013 | 7 | Politique ministérielle de défense et de sécurité ; Révision générale | Gerald Bartholomew<br>Luc Vallée | GB-LV | André Gariazzo |
| 23/05/2016 | 8 | Directive nationale de sécurité ; Révision générale | Gerald Bartholomew<br>Stéphane Dubreuil | GB-SD<br>CPDS<br>01/12/2015<br>CIDS<br>11/12/2015 | Éric Lucas |
| | | PES comptes à privilèges | Samuel Michel | | Premier ministre |
| | | PES cryptographie | Frédéric Loffredo | | |
| | | PES mise au rebut | Michaël Kiefer | | |
| 18/08/2016 | 9 | Polilitique ministérielle de défense et de sécurité ; Révision générale | Gerald Bartholomew<br>Stéphane Dubreuil<br>Jane Rain<br>Ana Ferreira | GB-SD-JR<br>CPDS<br>05/07/2016 | Éric Lucas |

# 1 ENJEUX DU SECTEUR

## *1.1 Présentation générale*

Le secteur d'activités d'importance vitale des activités judiciaires (SAIVAJ) se compose des entités suivantes :

### 1.1.1 Le ministère de la justice[1]

#### 1.1.1.1 Cabinet et secrétariat général

- Le cabinet du ministre assiste le ministre dans ses fonctions ;
- Le secrétariat général assiste le ministre, en liaison avec les directions, dans la définition et la mise en œuvre de la stratégie de modernisation du ministère, de son organisation territoriale et de sa politique de gestion des ressources humaines. Il est responsable des ressources humaines et des affaires financières du ministère de la justice. Le secrétaire général assume par ailleurs les fonctions de haut fonctionnaire de défense et de sécurité du SAIVAJ et est responsable à ce titre de la politique de défense et de sécurité.

#### 1.1.1.2 Les directions législatives

- La direction des affaires criminelles et des grâces exerce les attributions du ministère de la justice en matière pénale, en particulier en ce qui concerne l'évolution du droit pénal et le casier judiciaire ; elle développe son expertise en matière de politique pénale générale et spécialisée et apporte son soutien aux juridictions en mettant à leur disposition son analyse technique ; elle conçoit et assure le suivi de la normalisation des données pénales, ainsi que la gestion des bases de données juridiques des infractions pénales ; elle est en charge des négociations européennes et internationales dans ses domaines de compétence, ainsi que de l'entraide pénale internationale. Enfin, à travers l'activité du service du casier judiciaire national qui lui est directement rattaché, elle est garante de la mémorisation et de la restitution des condamnations prononcées ;
- La direction des affaires civiles et du sceau élabore les projets de réforme législative et réglementaire en matière de droit privé et concourt à l'élaboration du droit public et constitutionnel. Elle exerce la tutelle des professions judiciaires et juridiques soumises au contrôle de la Chancellerie. En matière civile et commerciale, elle élabore en liaison avec le service des affaires européennes et internationales les textes nécessaires à la mise en œuvre, au plan interne, des conventions d'entraide judiciaire internationale. Dans les matières relevant de sa compétence, elle conseille les autres administrations publiques et connait, en liaison avec le service des affaires européennes et internationales (SAEI), des questions internationales.

#### 1.1.1.3 Les directions de réseau

- La direction des services judiciaires (DSJ) assure l'organisation et le bon fonctionnement de toutes les juridictions judiciaires ; elle gère la carrière des magistrats et des fonctionnaires des greffes ;

[1] Décret n° 2008-689 du 9 juillet 2008 modifié relatif à l'organisation du ministère de la justice.

- La direction de l'administration pénitentiaire (DAP) met en œuvre l'exécution des décisions judiciaires concernant les personnes qui font l'objet d'une mesure judiciaire restrictive ou privative de liberté ;
- La direction de la protection judiciaire de la jeunesse (DPJJ) est chargée, dans le cadre de la compétence du ministère de la justice, de l'ensemble des questions intéressant la justice des mineurs et de la concertation entre les institutions intervenant à ce titre.

#### 1.1.1.4 Les établissements publics à caractère administratif (EPA) sous tutelle du ministère de la justice

- L'École nationale de la magistrature (ENM) ;
- L'École nationale d'administration pénitentiaire (ENAP) ;
- L'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC), en double tutelle avec le ministère du budget ;
- L'Agence publique pour l'immobilier de la justice (APIJ) ;
- L'Établissement public du palais de justice de Paris (EPPJP) ;
- L'Établissement public d'exploitation du livre foncier informatisé (ÉPELFI) ;
- Le Conseil national des communes « Compagnon de la Libération » (anciennement Conseil de l'ordre de la Libération).

### 1.1.2 Le Conseil d'État

- Conseil du Gouvernement et du Parlement sur les projets de lois et d'ordonnances, avant que ceux-ci ne soient soumis au conseil des ministres, et sur les projets de textes réglementaires ;
- Juge traitant, au dernier échelon de la juridiction administrative, les recours dirigés contre les autorités publiques ;
- Gestionnaire des tribunaux administratifs et des cours administratives d'appel.

## *1.2 Interdépendances au sein du secteur, avec d'autres secteurs et à l'international*

### 1.2.1 Interdépendances au sein du SAIVAJ

Au sein du SAIVAJ se remarque au premier abord une interdépendance de fond entre les ordres de justice administrative et judiciaire, étroitement complémentaires pour la continuité du système juridique national et la protection des libertés.
Une forte interdépendance lie par ailleurs entre elles les différentes missions du ministère de la justice, en particulier :

- l'activité pénale et l'exécution des peines sont interdépendantes ;
- l'ensemble des activités du ministère dépendent de l'infrastructure des systèmes d'information placée sous la responsabilité du secrétariat général.

### 1.2.2 Interdépendances intersectorielles

Au niveau national, le SAIVAJ est dépendant d'autres « secteurs d'activités d'importance vitale », qui se sont également dotés d'une directive nationale de sécurité (DNS) :

- la DNS « Activités civiles de l'Etat », au titre du maintien de l'ordre public et du réseau interministériel de l'Etat (RIE) ;
- la DNS « Établissements de santé », indispensable au maintien du système de soins dans les établissements pénitentiaires ;
- la DNS « Communication électronique et Internet » pour le soutien du Réseau privé virtuel de la justice ;
- les DNS du secteur de l'énergie pour l'alimentation en énergie des établissements ;
- la DNS « Alimentation » et « Gestion de l'eau » pour la provision d'alimentation et d'eau dans les établissements pénitentiaires, mais aussi de l'ensemble des autres établissements ;
- la DNS « Transports terrestres » pour garantir le fonctionnement des moyens logistiques (délivrance des moyens de subsistance aux établissements pénitentiaires et déplacement des placés sous main de justice en cas d'évacuation).

### 1.2.3 Interdépendances à l'international

Au plan international, le secteur d'importance vitale « Activités judiciaires » est dépendant des institutions européennes et internationales mises en œuvre par des traités ratifiés par la France ; il est partie prenante à la mise en œuvre de l'entraide judiciaire internationale.

## *1.3 Contraintes sur le secteur d'activités*

### 1.3.1 Contraintes juridiques

Le dispositif doit être conforme à l'ensemble de la réglementation en vigueur, internationale, européenne et nationale.

### 1.3.2 Grands principes caractérisant le fonctionnement de la justice

- ***Les juridictions***

Les juridictions (juges, tribunaux et cours) sont les autorités chargées de dire le droit à l'occasion d'un litige particulier : la fonction juridictionnelle consiste dans l'acte par lequel le juge découvre, à l'occasion d'un litige, quelle règle de droit trouve à s'appliquer dans les circonstances concrètes du cas d'espèce qui lui est soumis. Littéralement, la *juris-dictio* consiste dans l'acte de dire le droit.

Cette définition permet de distinguer les décisions proprement juridictionnelles (les ordonnances, jugements et arrêts), d'autres types de décisions (administratives, disciplinaires, *etc*.). Seules les premières sont entourées des garanties relatives à l'exercice du pouvoir judiciaire.

Le fonctionnement des juridictions est ainsi entouré de garanties, rappelées par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : l'indépendance, l'impartialité, la légalité, l'existence d'une voie de recours.

Mais ces exigences sont aussi des critères : une autorité qui, par exemple, ne disposerait pas de garanties suffisantes d'indépendance ne pourrait se voir confier des attributions juridictionnelles, sous peine d'une sanction par la Cour européenne des droits de l'homme.

- ***Le palais de justice***

Le tribunal est le lieu où se rend la justice. Le premier geste de justice au sein des sociétés humaines est de délimiter un lieu, de circonscrire un espace propice à son accomplissement. Le palais de justice participe à l'instauration d'un temps judiciaire qui tient à distance l'indignation morale et la colère publique, constitue le cadre habituel du rituel judiciaire, et conditionne *in fine* l'adhésion des justiciables à la décision de justice.

- ***La permanence de la justice***

Depuis 1789, les cours et tribunaux sont fixes et permanents. La permanence signifie que le service de la justice est assuré de façon continue, y compris les jours fériés et les dimanches en cas d'urgence. En matière civile comme administrative, cette continuité est assurée par le juge des référés qui peut être saisi à tout moment. En matière pénale, une permanence est assurée.

- ***L'indépendance et l'impartialité du juge***

Ces garanties, essentielles pour le justiciable, lui assurent que lorsque le juge prend une décision, il applique la règle de droit sans se laisser influencer par des pressions extérieures, par ses propres opinions ou préjugés ou par les risques qu'il encourt. Le principe de l'indépendance de l'autorité judiciaire est affirmé par les dispositions de l'article 64 de la Constitution du 4 octobre 1958.

- ***L'appel et le double degré de juridiction***

Le droit de contester une décision de justice devant une autre juridiction par la voie de l'appel est une garantie pour le justiciable. Toutefois, la loi prévoit que, pour des litiges où l'intérêt en jeu est de faible importance, les jugements sont rendus « en premier et dernier ressort ». Dans cette hypothèse, seule la voie du pourvoi en cassation est ouverte.

- ***Le droit à un procès équitable***

En matière civile, ce principe signifie que le juge ne tranche un litige qu'après une libre discussion des prétentions et des arguments de chacune des parties. Il s'assure que les parties se communiquent entre elles les pièces du dossier. Il veille au respect du principe du contradictoire, qui impose que toute partie ayant un intérêt à défendre doit pouvoir être présente, valablement représentée ou dûment convoquée.

Sur le plan pénal, nul ne peut être poursuivi ou condamné pour des faits qui ne sont pas prévus, réprimés et punis d'une peine déterminée par la loi. A toutes les étapes de la procédure, le justiciable bénéficie de droits reconnus aux personnes poursuivies ou soupçonnées d'une infraction, notamment : droit à un avocat dès le début de la procédure, droit à un procès équitable dans le cadre de débats contradictoires, droit d'exercer des recours, *etc*.

- ***La publicité des décisions de justice***

La justice est publique, sauf les cas où la loi exige ou permet que les débats aient lieu à huis clos ou en chambre du conseil. Il s'agit là d'un principe, inséré dans les codes de procédure, et consacré par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cette publicité permet à tout citoyen de pouvoir vérifier dans quelles conditions les décisions de justice sont rendues.

- ***Le contrôle de l'application du droit***

Par l'intermédiaire du pourvoi en cassation, le justiciable non satisfait d'une décision rendue par une cour d'appel ou un tribunal statuant en dernier ressort, exerce un recours qui permet de vérifier que le droit a été correctement appliqué.

Il ne s'agit pas d'un nouveau procès. La cassation ne constitue pas un troisième degré de juridiction. Son rôle est de dire si la décision de justice a été prise dans des conditions conformes aux règles de droit.

- ***La motivation des décisions de justice***

Les juges ont l'obligation de motiver leur décision, c'est-à-dire d'expliquer les raisons de fait et de droit qui les ont conduits à décider comme ils l'ont fait. Ce principe ne s'applique pas aux décisions rendues par les cours d'assises, celles-ci étant rendues par des jurys populaires sur la base de leur intime conviction.

- ***L'accès au droit et à la justice***

Pour permettre à chacun d'être en mesure de mieux connaître ses droits et ses obligations, les faire valoir et les exécuter, a été créé un dispositif d'aide à l'accès au droit qui consiste à offrir à quiconque en a besoin divers services (information, orientation…) dans des lieux accessibles ( tribunaux, maisons de justice et du droit, mairies, antennes de quartier…).

Les magistrats ne sont pas rémunérés par les justiciables mais par l'État. Toutefois, ces derniers doivent prendre en charge les frais de procédure et les honoraires des auxiliaires de justice (avocat, huissier de justice, expert…). En principe, chaque personne prenant part à un procès supporte ses propres frais. Pour permettre à celles qui sont sans ressources ou dont les ressources sont modestes d'engager un procès, de se défendre ou de faire face à des frais dans le cadre d'une transaction amiable, la loi a créé une aide financière « l'aide juridictionnelle » prise en charge par l'État.

Quant à l'accès à la justice, il permet à chacun :

- de faire entendre sa cause, de faire examiner son affaire par un juge indépendant et impartial au sens de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'article 4 du code civil disposant par ailleurs que « *le juge qui refusera de juger, sous prétexte du silence, de l'obscurité ou de l'insuffisance de la loi, pourra être poursuivi comme coupable d'un déni de justice* » ;
- d'être jugé selon les mêmes règles de droit et de procédure applicables à tous ;
- de s'exprimer dans sa langue et, si nécessaire d'être assisté d'un traducteur ou d'un interprète en langage des signes ;
- de se faire assister et/ ou représenter par le défenseur de son choix.

### 1.3.3 Contraintes budgétaires

Les limites budgétaires sont fixées annuellement par la loi de finances.
Ces contraintes sont traditionnellement fortes sur le secteur des activités judiciaires, elles évoluent toutefois du fait des mesures d'abondement dont le secteur a bénéficié sur les derniers exercices.
Les systèmes d'information, qui tiennent une place de plus en plus stratégique dans la marche du secteur, souffrent d'un sous-dimensionnement structurel des ressources humaines de la sous-direction de l'informatique et des télécommunications (SDIT). Ce contexte a pu être mis en évidence par les inspections successives menées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

## 1.4 Identification des missions d'importance vitale du SAIVAJ

Le ministre de la justice assure en toutes circonstances la continuité de l'activité pénale ainsi que l'exécution des peines. Il concourt par la mise en œuvre de l'action publique et l'entraide judiciaire internationale, à la lutte pour les intérêts fondamentaux de la Nation (article L. 1142-7 du code de la défense).

Le ministre coordonnateur du SAIVAJ assure en outre :

- la continuité du règlement des litiges, en privilégiant la permanence de l'accès au juge des référés, et la prise en charge des contentieux les plus urgents ;
- la continuité de la protection des personnes particulièrement vulnérables ;
- la continuité des missions liées aux services de placement et aux permanences éducatives ;
- la continuité de l'activité consultative du Conseil d'Etat et de l'activité des juridictions administratives liées aux procédures d'urgence et à la protection des libertés fondamentales.

## 1.5 Processus et biens supports des missions du SAIVAJ

### 1.5.1 Processus portés par les entités du secteur d'activités d'importance vitale « Activités judiciaires »

#### 1.5.1.1 Processus dépendant du secrétariat général

Le secrétaire général :

- assiste le ministre, en liaison avec les directions, dans la définition et la mise en œuvre de la stratégie de modernisation du ministère, de son organisation territoriale et de sa politique de gestion des ressources humaines ;
- est responsable des ressources humaines et des affaires financières du ministère de la justice ;
- représente, en ces domaines, le ministre dans les instances interministérielles compétentes. Il est assisté par un secrétaire général adjoint, directeur ;
- coordonne les actions intéressant plusieurs directions et assure la synthèse des dossiers et documents stratégiques transversaux ;
- anime et coordonne l'action des responsables de programme de la mission justice et prépare les arbitrages ministériels dans le domaine budgétaire ;
- assure l'harmonisation de la politique de gestion des ressources humaines au sein du ministère de la justice ; il définit et met en œuvre la politique de l'encadrement supérieur ;
- met en œuvre la politique du ministère en matière de systèmes d'information et de systèmes et réseaux de télécommunication et assure le soutien des directions dans la réalisation des opérations d'investissement immobilier, notamment pour le compte des services judiciaires ;
- conçoit et coordonne les actions ayant pour objet l'information statistique du ministère et assure le suivi des contentieux du ministère de la justice ;
- est chargé des actions de coopération européenne et internationale et apporte son appui aux directions compétentes dans la négociation d'accords internationaux ;
- met en œuvre les politiques ministérielles d'accès au droit et à la justice et de l'aide aux victimes ;
- élabore et met en œuvre la politique de communication du ministère de la justice ;
- est en charge de la politique d'études et de recherche du ministère ;
- pilote la mise en œuvre de la plate-forme nationale des interceptions judiciaires.

En tant que haut fonctionnaire de défense et de sécurité du SAIVAJ, le secrétaire général du ministère de la justice veille à la conception et à la mise en œuvre des politiques de défense et de sécurité des différentes entités rattachées au SAIVAJ.

### 1.5.1.2 Processus dépendant de la direction des affaires criminelles et des grâces (DACG)

La direction des affaires criminelles et des grâces exerce les attributions du ministère de la justice en matière pénale. Dans ce cadre, la DACG doit :

- élaborer la législation et la réglementation en matière répressive et examiner, en liaison avec les départements ministériels concernés, tous les projets de normes comportant des dispositions pénales ;
- conduire, en associant le secrétariat général, les négociations européennes et internationales en matière répressive ;
- préparer les instructions générales d'action publique, coordonner et évaluer leur mise en application ;
- contrôler l'exercice de l'action publique par les parquets généraux et les parquets ;
- instruire les recours en grâce et préparer les mesures d'amnistie ;
- veiller à la mise en œuvre des conventions internationales en matière d'entraide judiciaire pénale ;
- effectuer l'enregistrement des décisions judiciaires et superviser le fonctionnement du casier judiciaire national.

La direction des affaires criminelles et des grâces assure en outre :

- le suivi de l'action publique ;
- le suivi de l'ensemble des questions relatives au traitement judiciaire des victimes et à l'aide aux victimes.

### 1.5.1.3 Processus dépendant de la direction des affaires civiles et du sceau (DACS)

La direction des affaires civiles et du sceau prépare les projets de réforme législative et réglementaire en matière de droit privé et concourt à l'élaboration du droit public et constitutionnel. Dans le cadre de ses missions, la DACS doit :

- élaborer les projets de loi et de règlement en toutes les matières qui n'entrent pas dans la compétence spéciale d'une autre direction ;
- remplir le rôle de conseil en droit privé des autres administrations publiques ;
- animer et contrôler l'action du ministère public en matière civile et suivre la formation de la jurisprudence ;
- exercer les attributions dévolues à la chancellerie en matière de nationalité et de sceau et en ce qui concerne la réglementation et le contrôle des professions judiciaires autres que les magistrats et les personnels des greffes, ainsi que des professions juridiques soumises à son contrôle ;
- assurer la mise en œuvre des conventions internationales en matière d'entraide judiciaire civile et conduire, en associant le secrétariat général, les négociations européennes et internationales intéressant la législation de droit privé ;
- contribuer, en liaison avec le secrétariat général, à l'application des autres conventions internationales et du droit européen.

### 1.5.1.4 Processus dépendant de la direction des services judiciaires (DSJ)

La direction des services judiciaires a pour mission l'organisation et le bon fonctionnement de toutes les juridictions judiciaires. Dans le cadre de ses missions, la DSJ doit donc assurer la continuité :

- ***de l'activité pénale essentielle au maintien de l'ordre public :***

– les audiences de cours d'assises ;
– les audiences correctionnelles ;
– les audiences de comparution immédiate ;
– les présentations devant le juge d'instruction et le juge des libertés et de la détention ;
– les audiences du juge de l'application des peines ;
– les audiences du juge pour enfant ;
– les audiences de la chambre de l'instruction pour la détention ;
– les audiences de la chambre des appels correctionnels ;
– les audiences de la chambre de l'application des peines ;
– les permanences du parquet ;

- ***du traitement des contentieux civils :***

– les référés devant le tribunal de grande instance visant l'urgence, et les mesures urgentes relevant du juge aux affaires familiales (immeubles menaçant ruine, éviction conjoint violent, *etc*.) ;
– les audiences auprès d'un juge des libertés et de la détention civil (hospitalisation sous contrainte, rétention des étrangers) ;
– les référés visant la condition d'urgence au tribunal d'instance ;
– les permanences au tribunal pour enfants, l'assistance éducative d'urgence ;
– les référés devant le tribunal de commerce ;
– les référés prudhommaux.

- ***de l'activité de la Cour de cassation.***

#### 1.5.1.5 Processus dépendant de la direction de l'administration pénitentiaire (DAP)

La direction de l'administration pénitentiaire a pour mission la prise en charge des personnes placées sous-main de justice (PPSMJ). Dans le cadre de ses missions, la DAP doit :

- ***assurer la continuité de l'activité du greffe pénitentiaire :***

– éviter la rupture de l'activité pénale et de la mise à exécution des peines prononcées ;

- ***éviter le risque de détentions arbitraires et de libérations anticipées ; assurer la garde des populations placées sous main de justice (PPSMJ) en milieu fermé :***

– éviter les risques de troubles à l'ordre public ;

- ***assurer l'entretien des PPSMJ en milieu fermé :***

– assurer l'alimentation et l'hydratation des PPSMJ ;
– assurer les soins des détenus malades et non pris en charge ;
– circonscrire toute propagation de maladies infectieuses contagieuses (type gale, *etc*.) ;

- ***assurer la surveillance et le suivi des PPSMJ en milieu ouvert :***

– conserver la supervision des PPSMJ placés sous surveillance électronique ;
– prévenir la récidive et protéger les victimes en garantissant un périmètre d'exclusion entre les PPSMJ placées et elles ;
– permettre la réinsertion des PPSMJ en proposant une alternative à l'incarcération, notamment pour les détenus condamnés à de courtes peines ;

- éviter la commission d'infractions conduisant à une hausse des incarcérations (révocations de mesures) ayant pour conséquence un accroissement de l'activité pénale des tribunaux ;

  - ***assurer la continuité des services en charge du support :***

- garantir la disponibilité des ressources humaines dans les services pénitentiaires en assurant la continuité de la gestion des services administratifs (paie, gestion des effectifs et emplois, *etc*.) ;
- présence en nombre suffisants de personnels (d'encadrement, de surveillance et administratifs) pour assurer les différentes missions précédemment définies.

#### 1.5.1.6 Processus dépendant de la direction de la protection judiciaire de la jeunesse (DPJJ)

La direction de la protection judiciaire de la jeunesse est chargée de l'ensemble des questions intéressant la justice des mineurs et de la concertation entre les institutions intervenant à ce titre. Dans le cadre de ses missions, la DPJJ doit :

- concevoir les normes et cadres d'organisation de la justice des mineurs (en relation avec les directions compétentes) ;
- garantir directement, ou par son secteur associatif habilité, une aide aux décisions de l'autorité judiciaire ;
- assurer directement, dans les services et établissements de l'Etat, la prise en charge de mineurs placés sous-main de justice ;
- garantir à l'autorité judiciaire, par le contrôle, l'audit et l'évaluation, la qualité de l'aide aux décisions et celle de la prise en charge quel que soit le statut des services et établissements sollicités ;
- définir et conduire, en liaison avec le secrétariat général, la politique des ressources humaines menée au profit des personnels des services déconcentrés et élaborer les règles statutaires applicables aux corps propres à la protection judiciaire de la jeunesse ;
- développer les outils de gestion prévisionnelle ;
- assurer un suivi individualisé des carrières ;
- conduire la politique de formation mise en œuvre par l'Ecole nationale de protection judiciaire de la jeunesse (ENPJJ) ;
- déterminer les objectifs stratégiques et opérationnels, définir les besoins de fonctionnement et d'équipements, répartir les ressources et les moyens entre les différents responsables fonctionnels et territoriaux.

#### 1.5.1.7 Processus dépendant de l'inspection générale des services judiciaires (IGSJ)

L'inspection générale des services judiciaires a pour mission l'inspection de l'ensemble des directions et services du ministère de la justice, ainsi que des juridictions de l'ordre judiciaire et des personnes morales de droit public ou privé dont les activités sont liées à celles du ministère. Dans le cadre de ses missions, l'IGSJ doit :

- évaluer le fonctionnement et la performance des entités qui relèvent de son périmètre ;
- réaliser les enquêtes administratives initiées par saisine du ministre ;
- assurer le conseil du garde des sceaux sur la faisabilité ou les impacts d'une réforme en lien avec les politiques publiques ;
- conduire les audits et le contrôle interne permanent au sein du ministère.

### 1.5.1.8 Processus dépendant du Conseil d'État

Le Conseil d'État a pour mission d'assurer l'activité consultative auprès du gouvernement et l'activité juridictionnelle administrative. Dans le cadre de ses missions, le Conseil d'État doit :

- ***conseiller le Gouvernement :***

– en application de l'article 39 de la Constitution, le Conseil d'État est obligatoirement saisi des projets de loi, avant leur adoption par le Conseil des ministres et leur dépôt devant le Parlement ;
– en vertu de l'article 38 de la Constitution, il doit être saisi des projets d'ordonnance avant leur adoption par le Conseil des ministres ;
– les décrets en Conseil d'État ne peuvent être pris ou modifiés qu'après saisine du Conseil d'Etat ;
– les projets d'actes communautaires qui sont adressés au Gouvernement par la Commission sont examinés par le conseil qui distingue les dispositions qui relèveraient en droit national de l'article 34 de la constitution et qui doivent être transmises pour avis au Parlement ;
– sur toute question posant un problème juridique particulier ;

- ***assurer l'activité juridictionnelle :***

– tous les litiges qui impliquent une personne publique (l'État, les régions, les collectivités territoriales, les établissements publics) ou une personne privée chargée d'un service public (comme les ordres professionnels, les fédérations sportives) relèvent, sauf si une loi en dispose autrement, de la compétence des juridictions administratives et donc, en dernier ressort, du Conseil d'État ;
– juge de cassation des arrêts des cours administratives d'appel et des juridictions administratives spécialisées et assure l'unité de la jurisprudence sur le plan national ;
– juge en premier et dernier ressort des recours dirigés notamment contre les décrets, les actes réglementaires des ministres, les actes des organismes collégiaux à compétence nationale, le contentieux des élections régionales et de l'élection des représentants français au Parlement européen ;
– juge en appel pour les contentieux des élections municipales et cantonales ;

- ***entretenir le réseau des juridictions administratives ;***
- ***assurer la mission permanente d'inspection des juridictions administratives qui contrôle le bon fonctionnement des juridictions.***

### 1.5.1.9 Processus dépendant de l'agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC)

L'Agence de gestion et de recouvrement des avoirs saisis et confisqués a pour mission de faciliter la saisie et la confiscation en matière pénale[2].

- ***Dans le cadre de ses missions l'AGRASC doit :***

– assurer la gestion centralisée, sur un compte qu'elle a ouvert à la Caisse des dépôts et consignations, de toutes les sommes saisies (c'est-à-dire appréhendées dans l'attente d'un jugement définitif, en vue d'une éventuelle confiscation) lors de procédures pénales en France (2° de l'article 706-160 du code de procédure pénale) ;

[2] Article 4 de la loi n° 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale.

- procéder à l'ensemble des ventes avant jugement de biens meubles saisis, décidées par les magistrats lorsque ces biens meubles ne sont plus utiles à la manifestation de la vérité et qu'ils sont susceptibles de dépréciation ;
- assurer l'ensemble des publications, auprès des bureaux de conservation des hypothèques, des saisies pénales immobilières (article 706-151 du code de procédure pénale). L'agence est également chargée, conformément aux dispositions de l'article 707-1 du code de procédure pénale, de la publication des confiscations immobilières prononcées par les juridictions ;
- gérer, sur mandat de justice, tous les biens complexes qui lui sont confiés, c'est-à-dire tous les biens qui nécessitent, pour leur conservation ou leur valorisation, des actes d'administration (1° de l'article 706-160 du code de procédure pénale) ;
- gérer les biens saisis, procéder à leur vente et à la répartition du produit de la vente en exécution de toute demande d'entraide internationale ou de coopération émanant d'une autorité judiciaire étrangère (4° de l'article 706-160 du code de procédure pénale) ;
- veiller, enfin, le cas échéant, à l'information préalable des créanciers (créanciers publics ou victimes) avant exécution de toute décision judiciaire de restitution (alinéa 4 de l'article 706-161 du code de procédure pénale) et à l'indemnisation prioritaire des parties civiles sur les biens confisqués à la personne condamnée (article 706-164).

#### 1.5.1.10 Processus dépendant de l'agence publique pour l'immobilier de la justice (APIJ)

L'agence publique pour l'immobilier de la justice a pour mission la conception et la gestion des grands projets immobiliers relevant du ministère. Dans le cadre de cette mission l'APIJ doit construire, rénover et réhabiliter les palais de justice, les établissements pénitentiaires, les bâtiments de la protection judiciaire de la jeunesse, les écoles de formation du ministère, en France métropolitaine et en outre-mer.

#### 1.5.1.11 Processus dépendant de l'établissement public du palais de justice de Paris (EPPJP)

L'établissement public du palais de justice de Paris a pour mission de pallier la dissémination des juridictions du palais de justice de Paris et leur mauvais état technique. Dans le cadre de cette mission l'EPPJP doit :
- concevoir, acquérir, faire construire et aménager de nouveaux locaux plus adaptés aux besoins des juridictions ;
- procéder au réaménagement du bâtiment historique de l'île de la Cité.

#### 1.5.1.12 Processus dépendant de l'établissement public d'exploitation du livre foncier informatisé (ÉPELFI)

L'établissement public d'exploitation du livre foncier informatisé a pour mission de détenir et d'entretenir le livre foncier « Alsace-Moselle ». Dans le cadre de cette mission l'ÉPELFI doit :
- assurer l'exploitation du système informatique AMALFI (Alsace-Moselle application pour un livre foncier informatisé) ;
- garantir la sécurité du système et des données inscrites au livre foncier ;
- fixer le montant de la redevance d'accès aux services.

#### 1.5.1.13 Processus dépendant de l’École nationale de la magistrature (ENM)

L’École nationale de la magistrature a pour mission de :

- assurer la formation initiale et continue les auditeurs de justice ;
- contribuer à la formation des magistrats d’Etats étrangers.

#### 1.5.1.14 Processus dépendant de l’École nationale d’administration pénitentiaire (ENAP)

L’École nationale d’administration pénitentiaire a pour mission de :

- assurer la formation initiale et continue des agents public occupant un emploi dans l’administration pénitentiaire ;
- réaliser des travaux de recherche et d’étude et les diffuser ;
- mettre en œuvre des actions de partenariat avec des institutions d’enseignement et de recherche françaises et étrangères.

#### 1.5.1.15 Processus dépendant du Conseil national des communes « Compagnon de la Libération »

Le Conseil national des communes « Compagnon de la Libération » a pour mission de :

- veiller à la pérennité des traditions de l'ordre de la Libération et de porter témoignage de celui-ci devant les générations futures, en liaison avec les unités combattantes titulaires de la Croix de la Libération ;
- mettre en œuvre toutes les initiatives qu'il juge utiles, dans les domaines pédagogique, muséographique ou culturel, en vue de conserver la mémoire de l'ordre de la Libération, de ses membres et des médaillés de la résistance française ;
- gérer le musée de l'ordre de la Libération et le maintenir, ainsi que les archives de l'ordre, en leurs lieux dans l'hôtel des Invalides ;
- organiser, en liaison avec les autorités officielles, les cérémonies commémoratives de l'appel du 18 juin et de la mort du général de Gaulle ;
- participer à l'aide morale et matérielle aux compagnons de la Libération, aux médaillés de la résistance française et à leurs veuves et enfants.

### 1.5.2 Infrastructures

#### 1.5.2.1 Sites de l’administration centrale

- Site Olympe de Gouges qui a vocation à héberger progressivement l’ensemble des services centraux parisiens, jusqu’alors répartis sur 11 sites ;
- 5 sites hébergeant les services centraux non parisiens ;
- les archives et entrepôts de Saint Fargeau ;
- les centres de production informatique de Nantes et Grigny ainsi que le centre télécom d’Amiens ;
- 9 plates-formes interrégionales réparties sur 12 sites.

### 1.5.2.2 Sites de l’autorité judiciaire

- Cour de cassation ;
- 36 cours d'appel ;
- un tribunal supérieur d'appel ;
- 161 tribunaux de grande instance (dont 16 à compétence commerciale) ;
- quatre tribunaux de première instance (dont deux à compétence commerciale) ;
- 155 tribunaux pour enfants ;
- 115 tribunaux des affaires de sécurité sociale ;
- 307 tribunaux d'instance et tribunaux de police ;
- 210 conseils de prud'hommes ;
- 6 tribunaux du travail ;
- 136 tribunaux de commerce.

### 1.5.2.3 Sites des services et établissements pénitentiaires

- 9 directions interrégionales des services pénitentiaires ;
- une mission des services pénitentiaires d’outre-mer ;
- 190 établissements pénitentiaires ;
- 58082 places en service [au 1er janvier 2015] ;
- 103 services pénitentiaires d’insertion et de probation (SPIP) ;

- ***Maisons d’arrêt :***

- 99 maisons d'arrêt [MA] ;
- 41 quartiers MA situés dans des centres pénitentiaires ;

- ***Établissements pour peine :***

- 25 centres de détention [CD] ;
- 37 quartiers [QCD] ;
- 46 centres pénitentiaires [CP] ;
- 6 maisons centrales [MC] ;
- 5 quartiers [QMC] ;
- 11 centres de semi-liberté autonomes [CSL] ;
- 10 quartiers [QSL] ;
- 7 quartiers pour peines aménagées [QPA] ;
- 6 établissements pénitentiaires pour mineurs [EPM] ;
- un établissement public de santé national à Fresnes.

### 1.5.2.4 Sites des services et établissements de la protection judiciaire de la jeunesse

- ***Établissements et services :***

- directions interrégionales ;
- directions territoriales ;
- 17 centres éducatifs fermés [CEF] ;
- 33 établissements de placement éducatif [EPE] ;
- 31 établissements de placement éducatif et d'insertion [EPEI] ;

- 93 services territoriaux éducatifs de milieu ouvert [STEMO] ;
- 25 services territoriaux éducatifs de milieu ouvert et d'insertion [STEMOI] ;
- 3 services éducatifs auprès du tribunal [SEAT] ;
- 11 services territoriaux éducatifs et d'insertion [STEI] ;
- 6 services éducatifs au sein d'établissements pénitentiaires pour mineurs [SEEPM] ;
- un service éducatif au centre de jeunes détenus de Fleury-Mérogis [SECJD] ;

  - ***488 unités éducatives :***

- 17 unités éducatives centres éducatifs fermés [CEF] ;
- 4 unités éducatives centres éducatifs renforcés [UECER] ;
- 22 unités éducatives d'hébergement diversifié [UEHD] ;
- 74 unités éducatives d'hébergement collectif [UEHC] ;
- 267 unités éducatives de milieu ouvert [UEMO] ;
- 9 unités éducatives auprès du tribunal [UEAT] ;
- 85 unités éducatives d'activités de jour [UEAJ] ;
- 3 unités rattachées aux services éducatifs auprès des tribunaux [UESEAT] ;
- 6 unités des services éducatifs au sein d'établissements pénitentiaires pour mineurs [UESEEPM] ;
- une unité éducative au centre de jeunes détenus de Fleury-Mérogis [UECJD].

#### 1.5.2.5 Sites des juridictions administratives

- le Conseil d'État et ses annexes ;
- la Cour nationale du droit d’asile ;
- 8 cours administratives d'appel ;
- 42 tribunaux administratifs.

## *1.6 Principaux acteurs et critères de désignation des opérateurs d’importance vitale (OIV)*

***Conformément aux dispositions du code de la défense relatives à la protection des installations d’importance vitale :***

- tout service assurant l’une des missions d’importance vitale du SAIVAJ peut être désigné comme opérateur d’importance vitale sauf s’il apparaît qu’aucun de ses sites ne justifierait d’être désigné point d’importance vitale ;
- les établissements mettant en œuvre un processus identifié comme *« processus et biens supports des missions du secteur »* indispensable à un opérateur d’importance vitale pour se conformer à ses obligations d’importance vitale devront faire l’objet d’un classement comme point d’importance vitale (PIV) ;
- ces critères ne s’appliquent que pour engager la procédure de désignation, ils ne préjugent en rien la décision finale de désignation comme opérateur d’importance vitale ni de celle des points d’importance vitale au terme de l’analyse de risques décrite ci-dessous.

### 1.6.1 Activités à maintenir, éléments essentiels et opérateurs associés

- ***Un point d’importance vitale est un élément non substituable pour le fonctionnement de l’activité d’importance vitale, qui doit faire l’objet d’une protection spécifique, décrite au sein de la politique de défense et de sécurité du SAIV ;***

- ***Ces infrastructures comprennent :***

– des personnels indispensables à la continuité du SAIV, incluant des personnels internes et des intervenants externes ;
– des installations névralgiques abritant des activités sensibles ;
– des systèmes d'information composés d'applications et de moyens de traitement et de communication contribuant à la continuité de l'activité d'importance vitale.

### 1.6.2 Activités à maintenir dans chaque service

#### 1.6.2.1 Cabinet du Garde des sceaux

– continuité de la fonction, en assurant l'intendance et le processus d'élaboration des projets de loi et des textes réglementaires en liaison avec le secrétariat général du Gouvernement.

#### 1.6.2.2 Secrétariat général

- ***Le cabinet du secrétariat général :*** *mise en œuvre des missions propres au secrétaire général (voir 1.5.1.1).*
- ***La cellule d'appui du haut fonctionnaire de défense et de sécurité***

– contrôle de la mise en œuvre de la planification ministérielle de défense et de sécurité ;
– participation à la gestion interministérielle d'une crise.

- ***Les services du secrétaire général***

– gestion des sites de la Chancellerie et de l'administration centrale ;
– mise à disposition des agents des outils informatiques nécessaires à la conduite de leurs missions ;
– continuité de l'administration technique du réseau privé virtuel de la justice ;
– continuité du fonctionnement des centres de production informatique de données et de télécommunications ;
– continuité du pilotage des systèmes d'information et de télécommunication ;
– gestion du budget et des ressources humaines ;
– gestion de l'information liée à une communication de crise ;
– gestion des sites internet et intranet ;
– gestion administrative de l'aide aux victimes ;
– animation du réseau des magistrats en poste à l'étranger.

- ***La délégation des interceptions judiciaires en charge de la plate-forme nationale des interceptions judiciaires***

– continuité des interceptions au profit de l'autorité judiciaire.

#### 1.6.2.3 La direction des affaires criminelles et des grâces

– suivi de l'action publique, du traitement judiciaire des victimes et de l'aide aux victimes ;
– gestion de crise ;
– gestion du casier judiciaire national ;
– capacité d'élaboration en urgence d'un cadre normatif pénal ;
– exécution des mandats d'arrêt européens et des commissions rogatoires internationales ;
– enregistrement des décisions judiciaires.

#### 1.6.2.4 La direction des affaires civiles et du sceau

- capacité d'élaboration en urgence d'un cadre normatif civil et constitutionnel.

#### 1.6.2.5 La direction des services judiciaires

- gestion de crise.

#### 1.6.2.6 La direction de l'administration pénitentiaire

- gestion de crise.

#### 1.6.2.7 La direction de la protection judiciaire de la jeunesse

- gestion de crise.

#### 1.6.2.8 Inspection générale des services judiciaires

- capacité d'inspection des juridictions et des services ;
- capacité d'évaluation des politiques publiques.

#### 1.6.2.9 Juridictions judiciaires

- activité pénale essentielle au maintien de l'ordre ;
- référés, traitement et jugement des contentieux civils ayant un caractère d'urgence ;
- protection des personnes les plus vulnérables ;
- missions liées aux services de placement ;

***A moyen terme, il est nécessaire de préserver une activité réduite de :***

- fonctionnement de la Cour de Cassation ;
- fonctionnement du Conseil supérieur de la magistrature.

#### 1.6.2.10 Etablissements pénitentiaires

- garde et entretien des personnes placées sous main de justice ;
- accueil des personnes en détention ;
- activité des services d'insertion et de probation.

#### 1.6.2.11 Services de la protection judiciaire de la jeunesse

- permanences éducatives auprès des juridictions ;
- structures d'hébergement collectif des secteurs public et associatif habilité (foyers d'action éducative, centres de placement immédiat, centres éducatifs renforcés, centres éducatifs fermés) ;
- accueil en lieux de vie et en famille d'accueil.

### 1.6.2.12 Le Conseil d'État et les autres juridictions administratives

- activités consultatives relatives aux décisions gouvernementales urgentes ;
- activités liées aux procédures d'urgence et à la protection des libertés fondamentales.

## 1.6.3 Opérateurs et éléments essentiels du SAIVAJ

| OPÉRATEUR | DOMAINE | ÉLÉMENTS ESSENTIELS |
|---|---|---|
| **SECRÉTARIAT GÉNÉRAL**<br><br>Chancellerie et administration centrale<br><br>Réseau privé virtuel de la justice (RPVJ) et système d'information | SITES | – Place Vendôme et le Millénaire ;<br>– Plateformes interrégionales ;<br>– Centres de production informatique. |
| | Personnel et système d'information associés | – Cabinet, secrétariat général, directions, personnels de commandement, permanence IGSJ, délégation aux interceptions judiciaires ;<br>– Infrastructures informatiques : exploitants, administrateurs des applications vitales pour les métiers ou les applications transverses, infogérance ;<br>– Personnels de maintenance, de coordination, de proximité, des services logistiques ;<br>– Personnels en contact avec la presse, personnels qui ont la capacité technique de mettre en ligne les informations. |
| **DIRECTION DES SERVICES JUDICIAIRES**<br><br>Autorité judiciaire | SITES | – Palais de justice de Paris et de l'Ile de France ;<br>– Palais de justice des cours d'appel et TGI de zone de défense et de sécurité et des villes relais ;<br>– Palais de justice des juridictions exposées. |
| | Personnel et système d'information associés | – Magistrats, fonctionnaires, avocats et auxiliaires de justice ;<br>– Applications vitales pour les métiers ;<br>– Moyens de communication : téléphonie (mobile, fixe), messagerie électronique, fax ;<br>– Réseau de transport de données (RPVJ) ;<br>– Serveurs de fichiers et postes bureautiques. |

| | | |
|---|---|---|
| **DIRECTION DE L'ADMINISTRATION PÉNITENTIAIRE**<br><br>Réseau des services et établissements pénitentiaires | SITES | – Directions interrégionales des services pénitentiaires ;<br>– Établissements pénitentiaires sensibles (métropole et outre-mer) ;<br>– Unités de consultation et de soins ambulatoires, unités hospitalières sécurisées interrégionales, services médico-psychologique régionaux, établissement public de santé national de Fresnes. |
| | Personnel et système d'information associés | – Direction et personnels d'encadrement, de surveillance, équipes régionales d'intervention et de sécurité (ERIS) ;<br>– Personnel de gestion délégué et systèmes d'information associés ;<br>– Applications vitales pour les métiers ;<br>– Moyens de communications : téléphonie, radiophonie des établissements ;<br>– Moyens de protection des établissements : alimentation énergétique, vidéosurveillance… |
| **DIRECTION DE LA PROTECTION JUDICIAIRE DE LA JEUNESSE**<br><br>Réseau des services et des établissements de la protection judiciaire de la jeunesse (PJJ) | SITES | – Palais de justice de zone de défense et de sécurité d'Ile-de-France, des villes relais (juridictions du premier degré) ;<br>– Structures d'hébergement collectif des secteurs public et associatif habilité (foyer d'action éducative, centre de placement immédiat, centres éducatifs renforcés, centres éducatifs fermés). |
| | Personnel et système d'information associés | – Personnels PJJ et secteur associatif ;<br>– Applications vitales pour les métiers ;<br>– Moyens de communication : téléphonie (mobile, fixe), messagerie électronique, fax ;<br>– Réseau de transport de données. |
| **CONSEIL D'ETAT**<br><br>Conseil d'État et réseau des cours administratives d'appel et des tribunaux administratifs | SITES | – Palais Royal et locaux situés dans le centre d'affaires du Louvre (CAL) ; Montreuil ; site Richelieu ;<br>– Cours administratives d'appel (8) ;<br>– Les tribunaux administratifs d'Ile-de-France (Paris, Cergy-Pontoise, Melun, Versailles). |
| | Personnel et système d'information associés | – Membres du Conseil d'État, agents du corps des tribunaux administratif (TA) et cours administratives d'appel (CAA), agents du Conseil d'Etat et agents de greffe ;<br>– Applications vitales pour les métiers ;<br>– Moyens de communication : téléphonie (mobile, fixe), messagerie électronique, fax ;<br>– Réseau de transport de données. |

# 2 ANALYSE DE RISQUE

*Le chapitre relatif à l'analyse de risque, figurant dans le texte de la directive nationale de sécurité des activités judiciaires est classifié « confidentiel défense » et ne peut donc être reproduit dans le présent document.*

# 3 LIGNE DIRECTRICE N°1 : ORGANISATION, MANAGEMENT DE LA SÉCURITÉ, RÉPARTITION DES RESPONSABILITÉS

## *3.1 Organisation de la politique de défense et de sécurité*

La politique de défense et de sécurité du secteur d'activités d'importance vitale des activités judiciaires (SAIVAJ) prend appui sur une organisation homogène, s'inscrivant dans une approche globale des risques, et reposant sur la mise en œuvre d'un système de management de la sécurité dont la vocation est de s'étendre à l'ensemble des éléments constitutifs du secteur d'activités.

### 3.1.1 Au niveau du secteur d'activités d'importance vitale des activités judiciaires (SAIVAJ)

La directive nationale de sécurité (DNS) définit les objectifs et les politiques de défense et de sécurité du SAIVAJ ainsi que la nature des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste, devant être prise en compte par les opérateurs d'importance vitale (OIV).

Elle est intégrée au sein du référentiel national de défense et de sécurité (RNDS) du SAIVAJ, centralisée par le haut fonctionnaire de défense et de sécurité (HFDS) qui comprend, outre la directive nationale de sécurité des activités judiciaire approuvée par le Premier ministre, les éléments suivants :

- la politique ministérielle de défense et de sécurité (PMDS), qui :
  - intègre les dispositions non classifiées de la DNS et les complète en tant que de besoin par des règles ministérielles s'appliquant à l'ensemble des opérateurs visés par la présente directive ;
  - fait l'objet d'une procédure de rédaction et de révision coordonnée par le HFDS et intégrant le concours du comité mensuel de pilotage de la défense et de la sécurité ; elle est approuvée par arrêté du ministre coordinateur ;
  - centralise les règles de sécurité des systèmes d'information s'appliquant aux opérateurs reliés au réseau privé virtuel de la justice (RPVJ) ainsi que les règles d'organisation de la défense et de la sécurité au sein du ministère de la justice et constitue à ce titre la première partie du plan de sécurité d'opérateur et du référentiel central de défense et de sécurité de ces opérateurs ;
  - intègre ou centralise en annexe l'ensemble des procédures d'exploitation de la sécurité (PES) ;
  - comporte deux parties : l'une non protégée et diffusée dans l'ensemble des services, l'autre classifiée au niveau *Confidentiel - Défense* ;

- la collection des études de sécurité conduites dans le cadre de la présente directive ;

- la collection des plans ministériels de défense et de sécurité que le ministère de la justice serait amené à mettre en œuvre.

### 3.1.2 Au niveau des opérateurs d'importance vitale (OIV)

#### 3.1.2.1 Désignation des OIV

Les OIV relevant du SAIVAJ sont les suivants :

- le secrétariat général, auquel sont associées les directions d'administration centrale, au titre de la Chancellerie, de l'administration centrale, et du réseau privé virtuel du ministère de la justice ;

- la direction des services judiciaires (DSJ), à laquelle sont associées la direction des affaires civiles et du sceau et la direction des affaires criminelles et des grâces, au titre du réseau des juridictions judiciaires ;
- la direction de l'administration pénitentiaire (DAP), au titre du réseau des services et des établissements pénitentiaires ;
- la direction de la protection judiciaire de la jeunesse (DPJJ), au titre du réseau des services et des établissements de la protection judiciaire de la jeunesse ;
- le Conseil d'État (CE) pour lui-même et pour les autres juridictions administratives.

#### 3.1.2.2 Planification de défense et de sécurité

Le référentiel de sécurité opérateur (RSO) comprend les éléments suivants :

– le plan de sécurité d'opérateur élaboré par un OIV en relation avec le HFDS pour définir, dans le cadre fixé par la DNS complétée de la PMDS, la politique générale de protection des points d'importance vitale (PIV) et du réseau de services et d'établissements dont il a la charge ;
– le référentiel complémentaire de défense et de sécurité (RCDS) qui intègre les dispositions non classifiées du PSO et les complète en tant que de besoin en relation avec le HFDS ; il comporte deux parties : l'une non protégée et diffusée dans l'ensemble des services, l'autre classifiée au niveau *Confidentiel - Défense* ;
– la collection des études de sécurité conduites dans le cadre du PSO ;
– la déclinaison pour l'opérateur de tout plan ministériel que le SAIVAJ serait amené à mettre en œuvre.

Le PSO des opérateurs d'importance vitale reliés au RPVJ intègre :

– en première partie, la PMDS qui centralise les règles de sécurité des systèmes d'information s'appliquant aux utilisateurs du réseau ainsi que les règles d'organisation de défense et de sécurité au sein du ministère de la justice ;
– en seconde partie, les règles de défense et de sécurité spécifiques aux opérateurs.

Le PSO, les versions successives du RCDS et les déclinaisons de planification font l'objet d'une procédure de rédaction et de révision coordonnée par le HFDS et intégrant le concours du comité mensuel de pilotage de la défense et de la sécurité ; ils sont approuvés, après avis de la commission interministérielle de défense et de sécurité des secteurs d'activité d'importance vitale, par arrêté du ministre coordinateur.

#### 3.1.2.3 Cas particulier des PSO SG, DSJ et DPJJ

Les règles de défense et de sécurité constituant la seconde partie du plan de sécurité d'opérateur d'importance vitale des PSO SG, DSJ et DPJJ sont intégrées dans la présente politique ministérielle, les règles spécifiques à l'un de ces opérateurs faisant l'objet d'une mention particulière.
La présente PMDS constitue donc un document commun avec :

– le PSO SG ;
– le PSO DSJ ;
– le PSO DPJJ.

### 3.1.3 Au niveau zonal

Les chefs de cour de zone de défense et de sécurité élaborent, en concertation avec les membres du comité zonal de défense et de sécurité des activités judiciaires, les éléments des plans zonaux relatifs au SAIVAJ

### 3.1.4 Au niveau des établissements

#### 3.1.4.1 Plan particulier de protection (PPP)

Les autorités responsables des établissements faisant l'objet d'un classement en PIV élaborent un plan particulier de protection soumis à l'agrément du préfet de département.

#### 3.1.4.2 Plan de protection externe (PPE)

Les autorités responsables des établissements faisant l'objet d'un classement en PIV concourent à la rédaction d'un plan de protection externe (PPE) établi à l'initiative du préfet.

#### 3.1.4.3 Plan de protection (PP)

Les autorités responsables des établissements qui ne font pas l'objet d'un classement en PIV élaborent un plan de protection (PP) qui sera communiqué au préfet de département.

#### 3.1.4.4 Plan de protection et d'intervention des établissements pénitentiaires qui ne sont pas désignés PIV

Conformément aux dispositions de l'article D. 266 du code de procédure pénale, le plan de protection et d'intervention des établissements pénitentiaires non désignés PIV est soumis à l'agrément du préfet de département.

#### 3.1.4.5 Cas des juridictions situées dans une ZDS n'incluant pas la cour d'appel dont elles relèvent

Dans les cas où la juridiction est située sur une zone de défense n'incluant pas la cour d'appel dont elle relève, le plan de protection est transmis à la cour d'appel, et à la cour d'appel de la zone de défense dont elle relève, la cohérence du plan devant être appréciée au niveau de la zone de défense.

#### 3.1.4.6 Documents complémentaires spécifiques aux services judiciaires

En sus des documents réglementaires, les services judiciaires doivent entretenir des outils d'évaluation et de gestion :

##### *3.1.4.6.1 Dossier sûreté*

- le dossier sûreté regroupe au sein de chaque juridiction l'ensemble des documents relatifs à la sûreté et constitue ainsi une véritable mémoire de la juridiction ; il doit comporter, à titre non exhaustif le recensement des incidents survenus ;
- la liste des dispositifs de sûreté du site ;
- les demandes budgétaires ;
- les devis et contrats relatifs à la sûreté ;
- les références des entreprises concernées ;
- les coordonnées des interlocuteurs en matière de sûreté ;
- le plan d'intervention et de continuation des activités en cas de crise ;
- le cas échéant, les études sûreté réalisées.

##### *3.1.4.6.2 L'étude sûreté*

L'étude permet de déterminer les actions de sûreté à mettre en œuvre. Son élaboration dans chaque juridiction est donc obligatoire. Elle est réalisée sous la responsabilité des chefs de juridiction et sous le contrôle des chefs de cour.
Ce diagnostic sûreté est également le point de départ du projet sûreté.

#### *3.1.4.6.3 Le projet sûreté*

Le projet sûreté consiste à définir le dispositif qu'il convient de mettre en œuvre dans la juridiction afin d'obtenir un niveau de sûreté satisfaisant.

#### *3.1.4.6.4 La liste des dispositifs de sûreté du site*

Elle énumère les différentes thématiques qui structurent le plan partiulier de protection ou le plan de protection ;

- sécurisation des accès de la juridiction ;
- dispositifs électroniques et protection : vidéo protection, télésurveillance, anti-intrusion, badges et codes d'accès ;
- dispositifs pour les détenus : dépôt, attente gardée, circuit des détenus ;
- salle(s) d'audiences, box, dispositif d'alarme/d'alerte ;
- service des pièces à conviction, sécurisation et surveillance des lieux ;
- service des archives, accès sécurisé et sécurisation du lieu.

#### *3.1.4.6.5 La fiche incident*

Tous les évènements survenus dans les juridictions liés à de la malveillance doivent être déclarés : altercations, agressions verbales ou physiques, vols, dégradations, introduction d'objets illicites ou dangereux dans la juridiction…Hors période de crise, la remontée d'information s'effectue via les correspondants de sûreté régionaux.

## *3.2 Management de la politique de défense et de sécurité*

### 3.2.1 Prédominance des règles du référentiel national de défense et de sécurité

Le référentiel national de défense et de sécurité est un document évolutif qui définit le socle minimal pour les règles touchant à la défense et à la sécurité des établissements relevant du SAIVAJ.

Pour tous les niveaux de responsabilité et de décision et pour tous les principes et les domaines d'application de ces règles (organisation et management, gestion des risques, aspects humains, sensibilisation, gestion des événements de sécurité, aspects techniques, *etc*.), les règles décrites dans les référentiels de sécurité opérateur et dans leurs déclinaisons zonales, interrégionales et locales ne peuvent que renforcer les règles du RNDS et en aucun cas les affaiblir.

### 3.2.2 Audits et contrôles de sécurité

Un programme annuel d'audit coordonné par le HFDS est mis en œuvre à la diligence du HFDS et des autorités qualifiées pour effectuer des mesures d'écart entre les référentiels intéressant l'ensemble des domaines participant à la politique de défense et de sécurité (sûreté, sécurité, hygiène et santé, SSI) et la mise en œuvre réelle des mesures au sein des services.

### 3.2.3 Dispositifs de management obligatoirement inclus dans les PSO

- Réunions périodiques de revues de système permettant d'actualiser les référentiels ;

- Prise en compte des chaînes fonctionnelles des délégués à la défense et à la sécurité, officiers de sécurité, (central, zonaux et locaux, ou de projets) et des responsables SSI (central, zonaux, locaux, ou de projets) ;
- Procédures de remontée systématique à la direction et au HFDS, pour information, des événements de sécurité permettant d'opérer la prise en compte du retour d'expérience ;
- Systèmes d'audits périodiques de sécurité, permettant de mesurer les écarts entre la PSO et la pratique observée dans les établissements et de mettre en oeuvre des mesures correctives ;
- Procédures d'information périodique de la cellule d'appui du HFDS des projets du service susceptibles d'avoir des conséquences sur la politique de défense et de sécurité.

## *3.3 Répartition des responsabilités*

### 3.3.1 Le haut fonctionnaire de défense et de sécurité[3]

#### 3.3.1.1 Préparation des politiques de sécurité

Conformément aux dispositions du code de la défense, le HFDS est responsable de la planification de défense et de sécurité ainsi que de l'élaboration et de l'animation du système de management de la politique de défense et de sécurité, qui sont déclinées sous son autorité par les opérateurs et les autorités hiérarchiques rattachés au secteur d'activités d'importance vitale des activités judiciaires.

##### *3.3.1.1.1 Comité national de défense et de sécurité des activités judiciaires*

Le HFDS réunit en tant que de besoin le comité national de défense et de sécurité des activités judiciaires (CNDSAJ) composé des autorités qualifiées des opérateurs d'importance vitale, des chefs de cour de zone de défense et de sécurité et des représentants des échelons zonaux des opérateurs d'importance vitale.

##### *3.3.1.1.2 Comité de pilotage de la défense et de la sécurité*

Le HFDS réunit sur un rythme mensuel le comité de pilotage de la défense et de la sécurité (CPDS) composé des autorités qualifiées des opérateurs d'importance vitale, des chefs de cour de zone de défense et de sécurité et des représentants des échelons interrégionaux des opérateurs d'importance vitale.

Le CPDS :

– examine l'ensemble des contributions des services relatives aux évolutions des planifications nationales ou locales de défense et de sécurité : directive nationale de sécurité, politique ministérielle de défense et de sécurité, plans de sécurité d'opérateur, référentiels de défense et de sécurité, procédures d'exploitation de la sécurité, plans de continuité d'activité, plans particuliers de protection, *etc.* ;
– effectue un suivi des travaux des groupes de travail *ad hoc* constitués pour préparer des planifications particulières relevant de l'administration centrale ou des services déconcentrés ;
– tient à jour un observatoire permanent des systèmes d'information ; piloté par la la cellule d'appui du HFDS avec le concours de la SDIT sur la base des fiches fournies à un rythme mensuel par la maîtrise d'ouvrage et la maîtrise d'œuvre, cet observatoire a pour mission de tenir à jour un tableau

[3] Articles R. 1143-1 à R. 1143-8 du code de la défense.

de bord des systèmes d'information et des projets de systèmes d'information en cours ou envisagés et de suivre leur évolution dans le temps ;
- procède à la revue de contrôle mensuelle des incidents de sûreté ayant affecté les services et les établissements ainsi que la sécurité des systèmes d'information ;
- propose au secrétaire général un programme annuel d'audit du dispositif de défense et de sécurité.

#### 3.3.1.2 Conduite opérationnelle des politiques de sécurité

Le HFDS coordonne au sein du SAIVAJ l'organisation de prévention de crise et de gestion de situation d'urgence.

Il organise en lien avec le cabinet, la DACG, et l'ensemble des directions d'administration centrale, la représentation permanente du ministre coordonnateur auprès de la cellule interministérielle de crise (CIC) et de la cellule interministérielle d'aide aux victimes (CIAV).

Il anime les trois réseaux qui constituent pour l'ensemble du SAIVAJ les vecteurs structurels de circulation de l'information de défense et de sécurité, dans le sens ascendant et descendant (voir. ligne directrice n°5) :

- le réseau des chefs de cabinet des directions d'administration centrale ;
- le réseau des secrétaires généraux des cours d'appel de zone de défense et de sécurité, qui animent eux-mêmes leur réseau zonal ;
- le réseau des chefs de service au sein du secrétariat général.

Il active si nécessaire en cas de crise ministérielle ou interministérielle une salle de crise (le centre opérationnel Justice) et organise la contribution des opérateurs d'importance vitale et des directions d'administration centrale à son fonctionnement.

Il coordonne la mise en œuvre des décisions prises au sein de la cellule de crise du Premier ministre, de la cellule interministérielle de crise et de la cellule interministérielle d'aide aux victimes.

Il prend en charge la communication d'alerte destinée aux services ou aux agents en situation de crise, notamment en cas d'attaque sur les systèmes d'information.

Le HFDS est chargé de l'organisation et du maintien en condition opérationnelle du dispositif ministériel de situation d'urgence (article R. 1143-5 du code de la défense). Il assume parallèlement la mise en œuvre des politiques de sécurité, et élabore en tant que de besoin des propositions d'adaptation du dispositif de défense et de sécurité.

### 3.3.2 Le secrétaire général du Conseil d'État, les directeurs des services désignés OIV

#### 3.3.2.1 Préparation des politiques de défense et de sécurité

Le secrétaire général du Conseil d'État et les directeurs des services désignés comme opérateurs d'importance vitale (OIV) élaborent en concertation avec les directions et services associés, dans la limite de leurs attributions et dans le cadre fixé par le référentiel national de sécurité du secteur d'activités d'importance vitale « activités judiciaires », le référentiel de sécurité opérateur.

Ils procèdent dans les mêmes conditions à la déclinaison des planifications ministérielles de défense et de sécurité.

#### 3.3.2.2 Conduite opérationnelle des politiques de défense et de sécurité

Le secrétaire général, le secrétaire général du conseil d'État et les directeurs d'administration centrale ayant autorité sur un opérateur d'importance vitale sont les autorités qualifiées responsables en matière de défense et de sécurité dans le secteur dont ils ont la charge.

En accord avec le haut fonctionnaire de défense et de sécurité, ils définissent la politique de sécurité opérateur et en fixent les objectifs, élaborent le PSO et le RSO, s'assurent que les contrôles internes de sécurité sont régulièrement effectués, organisent la sensibilisation et la formation du personnel aux questions de défense et de sécurité, mettent en œuvre les procédures réglementaires de sécurité prescrites pour l'habilitation des personnes et des entreprises contractuelles, ainsi que pour l'homologation des produits et des installations.

#### 3.3.2.3 Rôle du délégué central à la défense et à la sécurité et du responsable central de la sécurité des systèmes d'information

Sont chargés des fonctions de délégué central à la défense et à la sécurité :

- les chefs de cabinet du secrétariat général, de la direction des services judiciaires, de la direction de la protection judiciaire de la jeunesse ;
- le directeur de cabinet de la direction de l'administration pénitentiaire ;
- le directeur de l'équipement du Conseil d'Etat.

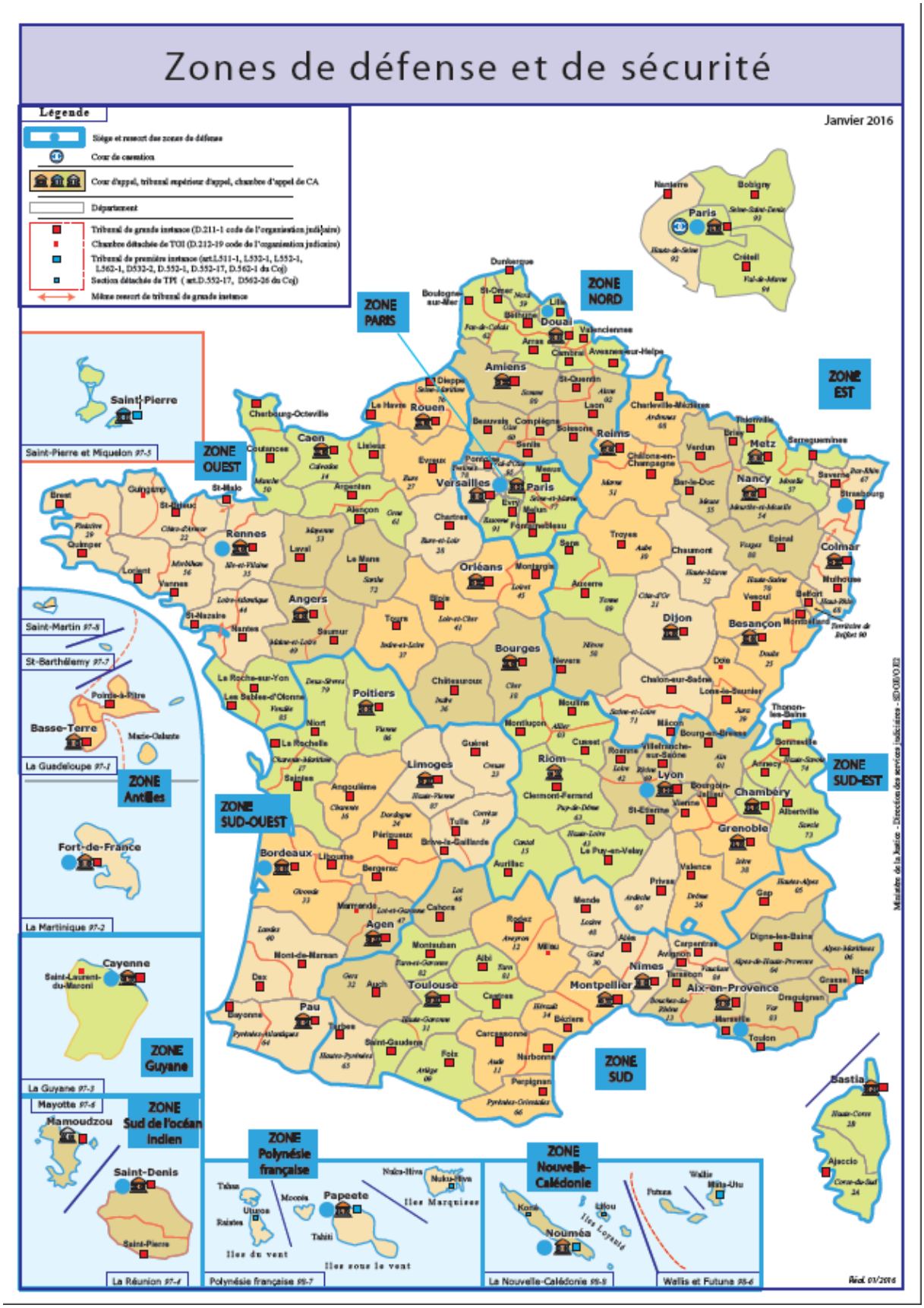
Le délégué central à la défense et à la sécurité représente l'opérateur d'importance vitale auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité ; il est assisté d'un responsable central de la sécurité des systèmes d'information (RCSSI), désigné par l'autorité qualifiée, pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.
Le délégué central à la défense et à la sécurité (DCDS) et le RCSSI animent la chaîne fonctionnelle de la défense et de la sécurité dans le périmètre de responsabilité de l'opérateur.
Maillons de la chaîne fonctionnelle ministérielle de défense et de sécurité, le DCDS et le RCSSI rendent compte de leurs travaux au HFDS (cellule d'appui du HFDS) ; ils apportent un concours actif au fonctionnement du comité mensuel de pilotage de la défense et de la sécurité.

Les personnes chargées des fonctions de DCDS et le RCSSI doivent être habilités au secret de la défense nationale.

### 3.3.3 Les chefs des cours d'appel du chef-lieu de la zone de défense et de sécurité

Conformément aux dispositions de l'article R. 122-24 du code de la sécurité intérieure, les chefs de cour d'appel dont le ressort couvre le chef-lieu de la zone de défense et de sécurité exercent les fonctions d'autorités correspondantes du ministre de la justice et des libertés, garde des sceaux, auprès du préfet de zone de défense et de sécurité. Ils animent et coordonnent la préparation et la mise en œuvre des politiques de défense et de sécurité des activités judiciaires et veillent à leur cohérence avec le dispositif zonal.

#### 3.3.3.1 Implantation des cours d'appel de zone de défense et de sécurité


Zones de défense et de sécurité
Janvier 2016
Légende
Siège et ressort des zones de défense
Cour de cassation
Cour d'appel, tribunal supérieur d'appel, chambre d'appel de CA
Département
Tribunal de grande instance (D.211-1 code de l'organisation judiciaire)
Chambre détachée de TGI (D.212-19 code de l'organisation judiciaire)
Tribunal de première instance (art.L.511-1, L.532-1, L.552-1, L.562-1, D.532-2, D.552-1, D.552-17, D.562-1 du Coj)
Section détachée de TPI (art.D.552-17, D.562-26 du Coj)
Même ressort de tribunal de grande instance
ZONE PARIS
ZONE NORD
ZONE EST
ZONE OUEST
ZONE SUD-OUEST
ZONE SUD-EST
ZONE SUD
ZONE Antilles
ZONE Guyane
ZONE Sud de l'océan Indien
ZONE Polynésie française
ZONE Nouvelle-Calédonie
Saint-Pierre et Miquelon 97-5
Saint-Martin 97-8
St-Barthélemy 97-7
La Guadeloupe 97-1
La Martinique 97-2
La Guyane 97-3
Mayotte 97-6
La Réunion 97-4
Polynésie française 98-7
La Nouvelle-Calédonie 98-8
Wallis et Futuna 98-6
Paris
Versailles
Lyon
Marseille
Toulouse
Bordeaux
Lille
Nantes
Strasbourg
Rennes
Fort-de-France
Cayenne
Saint-Denis
Mamoudzou
Papeete
Nouméa
Ministère de la Justice - Direction des services judiciaires - SDOEMO/EI
Actual. 01/2016

| IMPLANTATION DES COURS D'APPEL DE ZONE DE DÉFENSE ET DE SÉCURITÉ | | |
|---|---|---|
| **ZONE DE DÉFENSE ET DE SÉCURITÉ** | **SIÈGE DE LA COUR D'APPEL DE ZONE DE DÉFENSE ET DE SÉCURITÉ** | **TGI DU SIÈGE DE LA COUR D'APPEL DE ZONE DE DÉFENSE ET DE SÉCURITÉ** |
| **NORD** | DOUAI | LILLE |
| **PARIS** | PARIS | PARIS |
| **OUEST** | RENNES | RENNES |
| **SUD-OUEST** | BORDEAUX | BORDEAUX |
| **SUD** | AIX-EN-PROVENCE | MARSEILLE |
| **SUD-EST** | LYON | LYON |
| **EST** | COLMAR | STRASBOURG |
| **ANTILLES** | FORT-DE-FRANCE (responsabilité de la planification interzonale de défense et de sécurité Antilles-Guyane) | FORT-DE-FRANCE |
| **GUYANE** | | |
| **SUD DE L'OCÉAN INDIEN** | SAINT-DENIS-DE-LA-REUNION | SAINT-DENIS-DE-LA-REUNION |
| **NOUVELLE CALÉDONIE** | NOUMÉA | NOUMÉA |
| **POLYNESIE FRANCAISE** | PAPEETE | PAPEETE |

#### 3.3.3.2 Fonctions des chefs de cour d'appel de zone de défense et de sécurité

Les fonctions de chef de cour d'appel de zone de défense et de sécurité sont exercées *ès qualité* par les chefs de cour d'appel du chef-lieu de la zone de défense et de sécurité, et ne nécessitent donc pas la prise de l'arrêté ministériel prévu à l'article R.122-20 du code de la sécurité intérieure.

Ces fonctions échappent de même aux dispositions des articles R.122-21, R.122-22 et R.122-25 du code de la sécurité intérieure (direction et coordination de l'action des délégués par le préfet de zone de défense et de sécurité) ; l'action des chefs de cour, qui n'est pas dirigée par l'autorité préfectorale, doit cependant s'inscrire en cohérence avec le dispositif zonal défini par le préfet, les chefs de cour ayant mission de veiller à l'effectivité de cette cohérence.

Ces fonctions se rapportent à la préparation et à la mise en œuvre des politiques de défense et de sécurité, et recouvrent des actions de nature administrative exécutées sous l'autorité du ministre de la justice.

Elles s'exercent dans le périmètre des « activités judiciaires », entendues comme englobant, en application des dispositions de l'article L.1332-1 du code de la défense, l'ensemble des services du ministère de la justice présents dans la zone de défense et de sécurité (services judiciaires, pénitentiaires, de la protection judiciaire de la jeunesse, plates-formes interrégionales du ministère de la justice) ainsi que les juridictions administratives (tribunaux administratifs et cour administratives d'appel).

#### 3.3.3.3 Nature des fonctions exercées par les chefs de cour d'appel de zone de défense et de sécurité

La nature précise des fonctions exercées par les chefs de cour d'appel de zone de défense et de sécurité doit être interprétée au regard de l'article L.1142-7 du code de la défense, qui dispose que *« le ministre de la justice assure en toutes circonstances la continuité de l'activité pénale ainsi que l'exécution des peines* » et appelle donc à la mise en œuvre d'une politique de défense et de sécurité garantissant la résilience du secteur d'activités d'importance vitale des activités judiciaires.

Ce besoin de résilience s'étend au réseau des juridictions administratives pour les activités liées aux procédures d'urgence, à la protection des libertés fondamentales et aux reconduites à la frontière.

En application des articles R.1143-1 à R.1143-8 du code de la défense, la responsabilité du suivi de cette mise en œuvre est dévolue au niveau central, sous l'autorité du ministre, au haut fonctionnaire de défense et de sécurité, chargé d' *« animer et de coordonner au sein de son département la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence », de « sécurité des systèmes d'information* », d'en « *contrôler la préparation des mesures d'application* », et de « *s'assurer de l'élaboration et de la mise en œuvre des politiques de sécurité* » au sein des activités d'importance vitale.

Les dispositions introduites par l'article R.122-24 du code de la sécurité intérieure ont pour objectif, dans ce cadre, de relayer cette action au niveau déconcentré de la zone de défense et de sécurité, les attributions propres à la fonction de « chef de cour d'appel de zone défense et de sécurité » étant de même nature que celles dévolues au niveau central au haut fonctionnaire de défense et de sécurité, et s'exerçant dans le cadre défini par celui-ci.

#### 3.3.3.4 Préparation des politiques de défense et de sécurité

Les chefs de cour d'appel de zone de défense et de sécurité président conjointement avec le président de la juridiction administrative correspondante de la cour d'appel de zone de défense et de sécurité le comité zonal de défense et de sécurité des activités judiciaires (CZDSAJ) réunissant les chefs de cour d'appel, les présidents de cour administrative d'appel, les directeurs interrégionaux des services pénitentiaires, les directeurs interrégionaux de la protection judiciaire de la jeunesse, les coordonnateurs des plates-formes interrégionales du ministère de la justice.

Ils animent et coordonnent les travaux de planification de défense et de sécurité du SAIVAJ au niveau zonal et constituent à ce titre les interlocuteurs permanents du préfet de zone de défense et de sécurité, auxquels est associé, au titre de la justice administrative, le président de la juridiction administrative correspondant de la cour d'appel de zone de défense et de sécurité.

#### 3.3.3.5 Conduite opérationnelle des politiques de défense et de sécurité

Les chefs de cour d'appel de zone de défense animent et coordonnent la mise en œuvre des politiques de défense et de sécurité du SAIVAJ au niveau zonal ; ils vérifient la compatibilité des dispositions prises par les services et assurent la liaison entre les services relevant du SAIVAJ et le préfet de zone de défense ; ils effectuent une synthèse zonale des indicateurs de sécurité et disposent pour ce faire d'une cellule de liaison pourvue de systèmes protégés de communication.

#### 3.3.3.6 Rôle des secrétaires généraux au sein de cours d'appel de zone de défense et de sécurité

Conformément au schéma national de gestion des situations de crise arrêté à l'échelle du ministère de la justice (voir ligne directice n° 5), les secrétaires généraux auprès des chefs de cour de zone de défense et de sécurité assument de manière coordonnée la continuité des fonctions de délégué zonal à la défense et à la sécurité (DZDS).

Ils assistent à ce titre les chefs de cour de zone de défense et de sécurité dans la mise en œuvre de leurs responsabilités zonales et constituent le point de contact privilégié de l'ensemble des services déconcentrés du secteur d'activités d'importance vitale, comme du secrétariat général du ministère de la justice.

Ils ont vocation à représenter les chefs de cour de zone de défense et de sécurité auprès de l'autorité administrative pour toutes les questions relatives à la gestion de crise, à la sécurité des installations, ainsi qu'aux plans de défense et de sécurité.

Ils apportent leur concours aux chefs de cour de zone de défense et de sécurité pour la mise en œuvre des dispositions relatives à la sécurité de défense et à la protection du secret, et en contrôlent l'application au sein de la zone de défense et de sécurité.

Ils sont secondés en matière de sécurité des systèmes d'information et de télécommunication par un responsable zonal de la sécurité des systèmes d'information (RZSSI) ; ces fonctions ont vocation à être confiées au responsable de la gestion informatique (RGI), en liaison avec la cellule SSI du département informatique et télécommunication des plateformes interrégionales. Les RGI concernés bénéficient de formations prioritaires mises en place par la SDIT.

Ils coordonnent l'ensemble des intervenants de défense et de sécurité au sein des services judiciaires :

- les chargés de mission zonaux de défense et de sécurité : ces chargés se mission assistent les chefs de cour de zone de défense et de sécurité dans le cadre de leurs responsabilités, apportent leur concours aux secrétaires généraux du ressort de la zone de défense en matière de planification, contribuent à l'animation du comité zonal de défense et de sécurité et participent à la réalisation des diagnostics de sûreté ;
- les experts sûreté interrégionnaux (ESIR) : ces experts, installés administrativement auprès des chefs de cour siège de JIRS et sous l'autorité d'emploi des chefs de cour dans le ressort de laquelle ils sont missionnés, contribuent à l'élaboration des projets de sûreté des juridictions et des plans d'intervention et expertisent les actions dont le financement est demandé par les juridictions ;
- les correspondants sûreté régionaux et locaux : magistrats ou fonctionnaires désignés par les chefs de cour ou les chefs de juridiction, ils assistent ces derniers sur les questions relatives à la sûreté.

Les personnes chargées des fonctions de DZDS, de RZSSI, de chargé de mission zonal, d'ESIR, de correspondant sûreté, doivent être habilitées au secret de la défense nationale.

Le délégué zonal à la défense et à la sécurité et responsable zonal de la sécurité des systèmes d'information associent leurs homologues de la juridiction administrative (voir 3.3.8) lorsque celle-ci est concernée.

## Les chefs des cours d'appel

### 3.3.3.7 Rattachement des cours d'appel aux cours d'appel de zone de défense et de sécurité

| RATTACHEMENT DES COURS D'APPEL AUX COURS D'APPEL DE ZONE DE DÉFENSE ET DE SÉCURITÉ (CAZDS) | | |
|---|---|---|
| **ZONES DE DÉFENSE ET DE SÉCURITÉ** | **CAZDS** | **COURS D'APPEL RATTACHEES** |
| **NORD** | **DOUAI** | **DOUAI – AMIENS** |
| **PARIS** | **PARIS** | **PARIS – VERSAILLES** |
| **OUEST** | **RENNES** | **RENNES – ROUEN – CAEN – ANGERS – BOURGES – ORLEANS – VERSAILLES (au titre du TGI de CHARTRES) – POITIERS (au titre du TGI de La ROCHE sur YON et du TGI des SABLES d'OLONNE)** |
| **SUD-OUEST** | **BORDEAUX** | **BORDEAUX – POITIERS – LIMOGES – AGEN – PAU** |
| **SUD** | **Aix-en-Provence** | **AIX-EN-PROVENCE – NIMES – MONTPELLIER – TOULOUSE – AGEN (au titre du TGI de CAHORS et du TGI de AUCH) – PAU (au titre du TGI de TARBES) – GRENOBLE (au titre du TGI de GAP)** |
| **SUD-EST** | **LYON** | **LYON – RIOM – GRENOBLE – CHAMBERY – NIMES (au titre du TGI de PRIVAS)** |
| **EST** | **COLMAR** | **COLMAR – METZ – NANCY – REIMS - BESANÇON – DIJON – BOURGES (au titre du TGI de NEVERS) – PARIS (au titre du TGI d'AUXERRE)** |
| **ANTILLES** | **Fort-de-France** | **FORT-DE-FRANCE – BASSE-TERRE – CAYENNE** |
| **GUYANE** | | |
| **SUD DE L'OCÉAN INDIEN** | **SAINT-DENIS-de-la-REUNION** | **SAINT-DENIS-de-la-REUNION** |
| **NOUVELLE CALÉDONIE** | **NOUMÉA** | **NOUMÉA** |
| **POLYNESIE FRANCAISE** | **PAPEETE** | **PAPEETE** |

### 3.3.3.8 Préparation des politiques de défense et de sécurité

Les chefs des cours d'appel élaborent en concertation avec les juridictions placées sous leur autorité et avec l'ensemble des parties prenantes, dans la limite de leurs attributions et dans le cadre fixé par le référentiel de sécurité opérateur, les plans particuliers de protection des établissements désignés points d'importance vitale et les plans de protection des autres établissements.

Ils procèdent à la déclinaison, pour la cour d'appel, des planifications de défense et de sécurité dans le respect des orientations définies aux niveaux national et zonal des activités judiciaires.

#### 3.3.3.9 Conduite opérationnelle des politiques de défense et de sécurité

Les chefs des cours d'appel sont responsables de l'application des mesures définies par l'autorité qualifiée en matière de gestion de crise, de prévention de la malveillance et de sécurité des systèmes d'information.

#### 3.3.3.10 Rôle des secrétaires généraux au sein de cours d'appel

Conformément au schéma national de gestion des situations de crise arrêté à l'échelle du ministère de la justice (voir ligne directrice n° 5), les secrétaires généraux auprès des chefs de cour assument de manière coordonnée la continuité des fonctions de délégué à la défense et à la sécurité (DDS).

Ils assistent à ce titre les chefs de cour dans la mise en œuvre de leurs responsabilités en matière de défense et de sécurité et constituent le point de contact privilégié des secrétaires généraux auprès des chefs de cour de zone de défense et de sécurité, comme du secrétariat général du ministère de la justice.

Ils ont vocation à représenter les chefs de cour auprès de l'autorité administrative pour toutes les questions relatives à la gestion de crise, à la sécurité des installations, ainsi qu'aux plans de défense et de sécurité.

Ils apportent leur concours aux chefs de cour pour la mise en œuvre des dispositions relatives à la sécurité de défense et à la protection du secret, et en contrôlent l'application au sein des services judiciaires.

Ils sont secondés en matière de sécurité des systèmes d'information et de télécommunication par un responsable de la sécurité des systèmes d'information (RSSI) ; ces fonctions ont vocation à être confiées au responsable de la gestion informatique (RGI), en liaison avec la cellule SSI du département informatique et télécommunication des plateformes interrégionales. Les RGI concernés bénéficient de formations prioritaires mises en place par la SDIT.

Les chefs de cour procèdent en outre le cas échéant à la désignation d'un délégué à la défense et à la sécurité (DDS) au sein des autres établissements désignés points d'importance vitale, qui les représente auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité ainsi que d'un responsable de la sécurité des systèmes d'information (RSSI) chargé d'assister le délégué pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Ils font procéder au sein des autres établissements à la désignation d'un agent local de défense et de sécurité (ALDS) et d'un responsable local de la sécurité des systèmes d'information (RLSSI).

Les personnes chargées des fonctions de DDS, RSSI, ALDS et RLSSI doivent être habilitées au secret de la défense nationale.

### 3.3.4 Les directeurs interrégionaux des services pénitentiaires (DISP)

#### 3.3.4.1 Préparation des politiques de défense et de sécurité


L'ADMINISTRATION PÉNITENTIAIRE
Paris
Lille
Centre-Est - Dijon
Rennes
Est - Strasbourg
Lyon
Bordeaux
Toulouse
Marseille
Zone NORD
Zone PARIS
Zone OUEST
Zone EST
Zone SUD-OUEST
Zone SUD-EST
Zone SUD
Limite de direction interrégionale des services pénitentiaires
Limite départementale administrative
Maison d'arrêt (MA)
Centre de détention (CD)
Maison centrale (MC)
Centre de semi-liberté (CSL)
Centre pour peines aménagées (CPA)
Centre pénitentiaire (ici un quartier MA et un quartier SL)
Établissement pénitentiaire pour mineurs (EPM)
Centre national d'évaluation (CNE)
Établissement public de santé national (EPSN)
Unité hospitalière sécurisée interrégionale (UHSI)
Unité hospitalière spécialement aménagée (UHSA)
Siège de service pénitentiaire d'insertion et de probation (SPIP)
Antenne ou résidence administrative de SPIP
École nationale d'administration pénitentiaire (ENAP)
Service de l'emploi pénitentiaire (SEP)
Zones de défenses et de sécurité
Sièges des zones de défense
GUADELOUPE
GUYANE
MARTINIQUE
LA REUNION
MAYOTTE
Nouvelle-Calédonie
CP de Nouméa et SPIP
Polynésie française
SPIP
CD de Uturoa-Raiatea
CP de Faa'a Nuutania
CD de Taiohae-Marquises
Saint-Pierre-et-Miquelon
CP de Saint-Pierre-et-Miquelon
Wallis-et-Futuna
Mata-Utu : établissement placé sous l'autorité de la gendarmerie nationale
www.justice.gouv.fr
DAP/Service communication
Janvier 2016

Les directeurs interrégionaux des services pénitentiaires élaborent en concertation avec leurs services et avec l'ensemble des parties prenantes, dans la limite de leurs attributions et dans le cadre fixé par le référentiel de sécurité opérateur, les plans particuliers de protection des établissements désignés points d'importance vitale et les plans de protection des autres établissements.

Ils procèdent à la déclinaison pour la direction interrégionale, dans le cadre territorial des zones de défense et de sécurité et sous la coordination des chefs des cours d'appel de zone de défense et de sécurité, des planifications de défense et de sécurité.

#### 3.3.4.2 Conduite opérationnelle des politiques de défense et de sécurité

Les directeurs interrégionaux des services pénitentiaires sont responsables de l'application des mesures définies par l'autorité qualifiée en matière de gestion de crise, de prévention de la malveillance et de sécurité des systèmes d'information.

#### 3.3.4.3 Rôle du directeur interrégional adjoint, de l'officier inerrégional de sécurité et du responsable interrégional de sécurité des systèmes d'information

Au sein des directions interrégionales des services pénitentiaires, le directeur interrégional adjoint des services pénitentiaires (DIA-DISP), assume auprès du directeur interrégional les fonctions de délégué interrégional à la défense et à la sécurité ; il représente le directeur interrégional auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité ; il assure le lien avec les secrétaires généraux des cours d'appel de zone de défense et de sécurité dans le cadre des réseaux zonaux d'alerte et de gestion de crise.

L'officier interrégional de sécurité (OIS), placé sous l'autorité directe du DIA-DISP, est la personne ressource chargée de relayer la politique de défense et de sécurité et de coordonner les travaux de planification de défense et de sécurité dans le ressort de la direction interrégionale. Il relève de la chaîne fonctionnelle de défense et de sécurité coordonnée par l'officier central de sécurité de la DAP.

Le DIA-DISP est assisté par un responsable interrégional de la sécurité des systèmes d'information (RISSI) désigné par le directeur interrégional pour les questions de sécurité relatives aux systèmes d'information et de télécommunication qui relève de la chaîne fonctionnelle SSI placée sous la coordination du responsable central de la sécurité des systèmes d'information.

Les personnes chargées des fonctions de DIA-DISP, d'OIS et de RISSI doivent être habilitées au secret de la défense nationale.

#### 3.3.4.4 Désignation d'un délégué à la défense et à la sécurité et d'un responsable local de la sécurité des systèmes d'information au sein des établissements désignés points d'importance vitale

Les directeurs interrégionaux font procéder à la désignation d'un délégué à la défense et à la sécurité (DDS) au sein des établissements désignés points d'importance vitale, qui les représente auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité ; ils font désigner en outre un responsable local de la sécurité des systèmes d'information (RLSSI) chargé d'assister le délégué pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Dans les autres établissements, ils font procéder à la désignation d'un agent local de défense et de sécurité (ALDS) et d'un responsable local de la sécurité des systèmes d'information (RLSSI).

Les personnes chargées des fonctions de DDS, RLSSI, ALDS et RLSSI doivent être habilités au secret de la défense nationale.

### 3.3.5 Les directeurs interrégionaux de la protection judiciaire de la jeunesse

#### 3.3.5.1 Préparation des politiques de défense et de sécurité

Les directeurs régionaux de la protection judiciaire de la jeunesse élaborent en concertation avec leurs services et avec l'ensemble des parties prenantes, dans la limite de leurs attributions et dans le cadre fixé par le référentiel de sécurité opérateur, les plans de protection des établissements.

Ils procèdent à la déclinaison pour la direction interrégionale, dans le cadre territorial des zones de défense et de sécurité et sous la coordination des chefs des cours d'appel de zone de défense et de sécurité, des planifications de défense et de sécurité.

#### 3.3.5.2 Conduite opérationnelle des politiques de défense et de sécurité

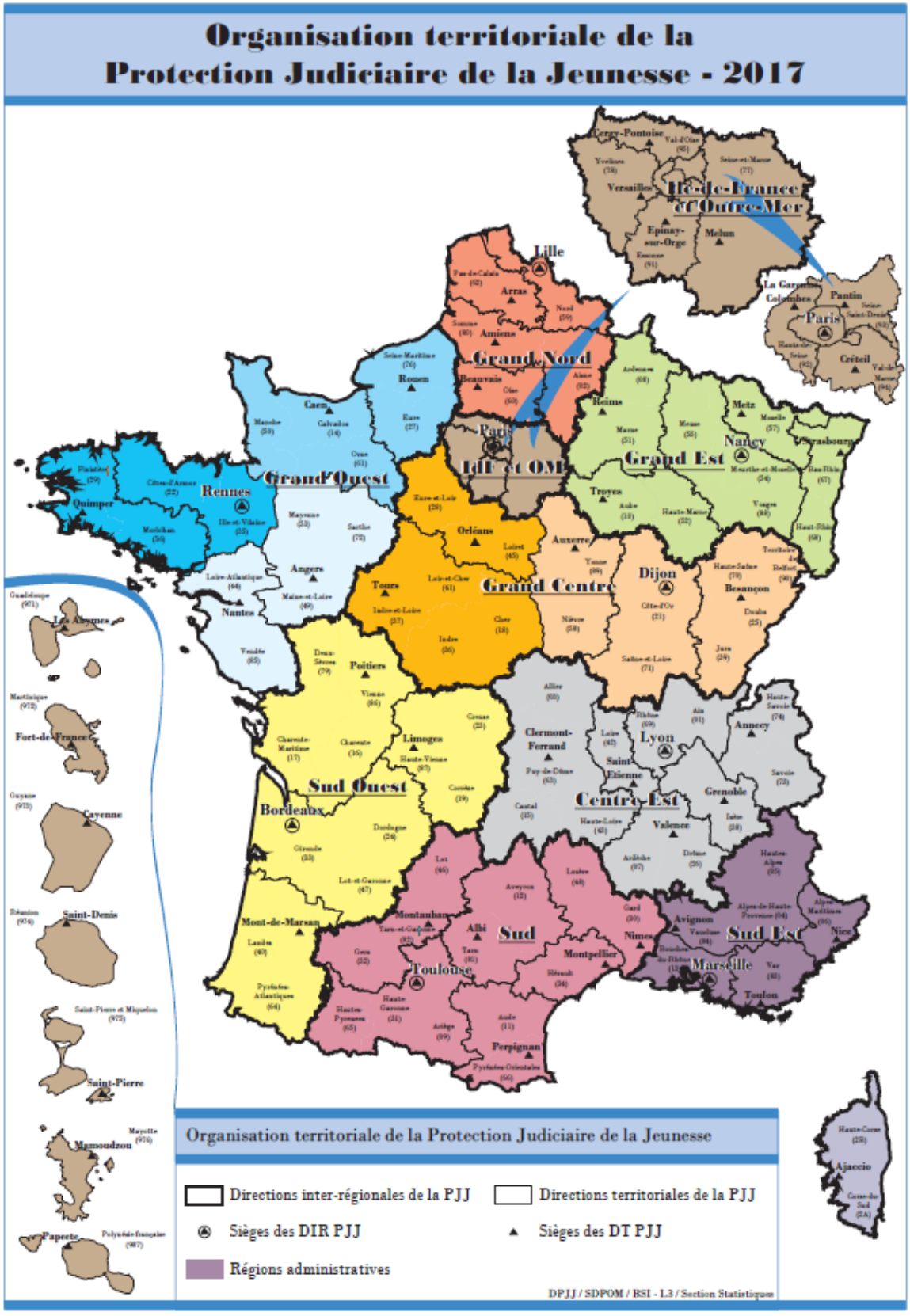
Les directeurs régionaux de la protection judiciaire de la jeunesse sont responsables de l'application des mesures définies par l'autorité qualifiée en matière de gestion de crise, de prévention de la malveillance et de sécurité des systèmes d'information.

#### 3.3.5.3 Rôle de l'adjoint au directeur interrégional et du responsable interrégional de la sécurité des systèmes d'information

Au sein des directions interrégionales de la protection judiciaire de la jeunesse, l'adjoint au directeur interrégional assume auprès du directeur interrégional, les fonctions de délégué interrégional à la défense et à la sécurité (DIDS) ; il représente le directeur interrégional auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité ; il assure le lien avec les secrétaires généraux des cours d'appel de zone de défense et de sécurité dans le cadre des réseaux zonaux d'alerte et de gestion de crise.

Il est assisté par un responsable interrégional de la sécurité des systèmes d'information (RISSI) désigné par le directeur interrégional pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Les personnes chargées des fonctions de DIDS et de RISSI doivent être habilitées au secret de la défense nationale.


Organisation territoriale de la
Protection Judiciaire de la Jeunesse - 2017
Ile-de-France et Outre-Mer
Grand Nord
Grand'Ouest
Grand Est
Grand Centre
Sud Ouest
Centre-Est
Sud
Sud Est
Rennes
Bordeaux
Dijon
Lyon
Nancy
Paris
Lille
Orléans
Tours
Poitiers
Limoges
Clermont-Ferrand
Grenoble
Annecy
Montpellier
Nîmes
Avignon
Marseille
Toulon
Nice
Toulouse
Perpignan
Pau
Nantes
Angers
Caen
Rouen
Amiens
Reims
Metz
Strasbourg
Besançon
Auxerre
Troyes
Ajaccio
Fort-de-France
Cayenne
Saint-Denis
Saint-Pierre
Mamoudzou
Papeete
Organisation territoriale de la Protection Judiciaire de la Jeunesse
Directions inter-régionales de la PJJ
Directions territoriales de la PJJ
Sièges des DIR PJJ
Sièges des DT PJJ
Régions administratives
DPJJ / SDPOM / BSI - L3 / Section Statistiques

### 3.3.6 Les coordonnateurs des plateformes interrégionales du ministère de la justice

#### 3.3.6.1 Implantation

| PLATES-FORMES INTERRÉGIONALES DU MINISTÈRE DE LA JUSTICE | | | |
|---|---|---|---|
| **PLATES-FORMES** | **RESSORT** | | |
| | **DSJ** | **DAP** | **DPJJ** |
| **LILLE** | CA DOUAI, AMIENS, ROUEN | DISP de LILLE | DIPJJ de LILLE |
| **NANCY** | CA NANCY, METZ, COLMAR, BESANÇON | DISP de STRASBOURG | DIPJJ de NANCY |
| **PARIS** | CA PARIS, VERSAILLES | DISP de PARIS | DIPJJ de PARIS (sauf outre-mer) |
| **DIJON** | CA DIJON, REIMS, ORLÉANS, BOURGES | DISP de DIJON | DIPJJ de DIJON |
| **LYON** | CA LYON, RIOM, CHAMBÉRY, GRENOBLE | DISP de LYON | DIPJJ de LYON |
| **RENNES** | CA RENNES, ANGERS, CAEN | DISP de RENNES | DIPJJ de RENNES |
| **TOULOUSE** | CA TOULOUSE, MONTPELLIER, AGEN, NÎMES | DISP de TOULOUSE | DIPJJ de TOULOUSE |
| **Aix-en-Provence** | CA AIX-EN-PROVENCE, BASTIA | DISP de MARSEILLE | DIPJJ de MARSEILLE |
| **BORDEAUX** | CA BORDEAUX, POITIERS, LIMOGES, PAU | DISP de BORDEAUX | DIPJJ de BORDEAUX |

Nota : les aires géographiques de compétence des départements de la plateforme peuvent différer ponctuellement de son aire officielle de compétence.

#### 3.3.6.2 Préparation des politiques de défense et de sécurité

Les coordonnateurs des plateformes interrégionales élaborent avec l'ensemble des parties prenantes, dans la limite de leurs attributions et dans le cadre fixé par la PMDS et les référentiels de sécurité opérateur, le plan de protection (PP) de leur établissement.

Ils procèdent à la déclinaison des planifications de défense et de sécurité dans le cadre territorial des zones de défense et de sécurité en concertation avec les chefs des cours d'appel de zone de défense et de sécurité.

#### 3.3.6.3 Conduite opérationnelle des politiques de défense et de sécurité

Les coordonnateurs des plateformes interrégionales sont responsables de l'application des mesures définies par les autorités qualifiées en matière de gestion de crise, de prévention de la malveillance et de sécurité des systèmes d'information.

#### 3.3.6.4 Désignation d'un délégué interrégional à la défense et à la sécurité et d'un responsable interrégional de la sécurité des systèmes d'information

Les coordonnateurs des plateformes interrégionales procèdent à la désignation d'un délégué à la défense et à la sécurité (DDS) qui les représente auprès de l'autorité administrative pour toutes les questions relatives à la gestion de crise, à la sécurité des installations et aux plans de défense et de sécurité ; le responsable de la cellule SSI du département informatique et télécommunication assiste le délégué pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Les personnes chargées des fonctions de DIDS et de responsable de la cellule SSI doivent être habilitées au secret de la défense nationale.

### 3.3.7 Les présidents de juridiction administrative correspondants des chefs de cour de zone de défense et de sécurité

#### 3.3.7.1 Implantation des juridictions administratives

| CONSEIL D'ÉTAT<br>(OPÉRATEUR D'IMPORTANCE VITALE) | | | |
|---|---|---|---|
| **IMPLANTATION DES JURIDICTIONS ADMINISTRATIVES<br>AU SEIN DES ZONES DE DÉFENSE ET DE SÉCURITÉ** | | | |
| **ZDS** | **CAZDS** | **Juridiction administrative de zone de défense et de sécurité** | **Autres juridictions administratives** |
| **NORD** | **DOUAI** | CAA DOUAI | TA LILLE |
| | | | TA AMIENS |
| **PARIS** | **PARIS** | CAA PARIS | COUR NATIONALE DU DROIT D'ASILE |
| | | | TA CERGY |
| | | | TA MELUN |
| | | | TA MONTREUIL |
| | | | TA PARIS |
| | | | CAA VERSAILLES |
| | | | TA VERSAILLES |
| **OUEST** | **RENNES** | CAA NANTES | TA CAEN |
| | | | TA NANTES |
| | | | TA ORLEANS |
| | | | TA RENNES |
| | | | TA ROUEN |
| **SUD-OUEST** | **BORDEAUX** | CAA BORDEAUX | TA BORDEAUX |
| | | | TA LIMOGES |
| | | | TA PAU |
| | | | TA POITIERS |
| | | | TA TOULOUSE |
| **SUD** | **AIX-EN-PROVENCE** | CAA MARSEILLE | TA BASTIA |
| | | | TA MARSEILLE |
| | | | TA MONTPELLIER |
| | | | TA NICE |
| | | | TA NIMES |
| | | | TA TOULON |

| | | | |
|---|---|---|---|
| **SUD-EST** | **LYON** | CAA LYON | TA CLERMONT-FERRAND |
| | | | TA GRENOBLE |
| | | | TA LYON |
| **EST** | **METZ** | CAA NANCY | TA BESANÇON |
| | | | TA CHALONS-EN-CHAMPAGNE |
| | | | TA DIJON |
| | | | TA NANCY |
| | | | TA STRASBOURG |
| **ANTILLES GUYANE** | **FORT-DE-FRANCE** | TA BASSE TERRE | TA FORT-DE-FRANCE |
| | | | TA SAINT-BARTHELEMY |
| | | | TA SAINT-MARTIN |
| | | | TA CAYENNE |
| **SUD OCÉAN INDIEN** | **SAINT-DENIS** | TA SAINT-DENIS-DE-LA-REUNION | TA MAMOUDZOU |
| **NOUVELLE CALÉDONIE** | **NOUMEA** | TA NOUMEA | TA MATA UTU |
| **POLYNÉSIE FRANÇAISE** | **PAPEETE** | TA PAPEETE | |

#### 3.3.7.2 Préparation des politiques de défense et de sécurité

Chaque chef de juridiction élabore avec l'ensemble des parties prenantes, dans la limite de ses attributions et dans le cadre fixé par le référentiel de sécurité opérateur, le plan particulier de protection (PPP) ou le plan de protection (PP) de son établissement, selon que celui-ci est désigné ou non point d'importance vitale (PIV).

Les présidents de juridiction administrative correspondants des chefs de cour d'appel de zone de défense et de sécurité assurent un rôle de coordinateur zonal pour l'élaboration de ces plans, en concertation avec chaque juridiction concernée.

Ils procèdent à la déclinaison des planifications de défense et de sécurité dans le cadre territorial des zones de défense et de sécurité en concertation avec les chefs des cours d'appel de zone de défense et de sécurité.

#### 3.3.7.3 Conduite opérationnelle des politiques de défense et de sécurité au niveau des cours administratives d'appel et des tribunaux administratifs

Les présidents des juridictions administratives sont responsables de l'application des mesures définies par le secrétaire général du Conseil d'État en matière de prévention de la malveillance et de sécurité des systèmes d'information.

#### 3.3.7.4 Désignation d'un délégué zonal à la défense et à la sécurité et d'un responsable zonal de sécurité des systèmes d'information

Le président de juridiction administrative correspondant des chefs de cour d'appel de zone de défense et de sécurité peut assurer lui-même, pour la juridiction administrative, les fonctions de délégué zonal à la défense et à la sécurité (DZDS), ou désigner ce délégué, qui le représente auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité.

Le DZDS assure le lien avec les secrétaires généraux des cours d'appel de zone de défense et de sécurité dans le cadre des réseaux zonaux d'alerte et de gestion de crise.

Le responsable régional des systèmes d'information de la juridiction administrative compétent est désigné responsable zonal de la sécurité des systèmes d'information (RZSSI) pour la juridiction administrative. Il est chargé d'assister le président de juridiction administrative correspondant du chef de cour d'appel de zone de défense ou le délégué désigné par ce président pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Les personnes chargées des fonctions de DZDS et de RZSSI doivent être habilitées au secret de la défense nationale.

#### 3.3.7.5 Désignation d'un délégué à la défense et à la sécurité et d'un responsable de la sécurité des systèmes d'information au sein des établissements désignés points d'importance vitale

Le président de chaque juridiction administrative désigne un délégué à la défense et à la sécurité (DDS) au sein des établissements désignés points d'importance vitale, qui les représente auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de défense et de sécurité.

Le correspondant informatique de chaque juridiction administrative est désigné responsable local de la sécurité des systèmes d'information (RLSSI) chargé d'assister le délégué pour les questions de sécurité relatives aux systèmes d'information et de télécommunication.

Pour les autres établissements, non désignés point d'importance vitale, le président de chaque juridiction administrative désigne un agent local de défense et de sécurité, et le correspondant informatique est désigné responsable local de sécurité des systèmes d'information.

Les personnes chargées des fonctions de DDS, RLSSI et d'ALDS doivent être habilitées au secret de la défense nationale.

# 4 LIGNE DIRECTRICE N° 2 : GARANTIR LA COHÉRENCE DES POLITIQUES DE DÉFENSE ET DE SÉCURITÉ

## *4.1 Globaliser l'approche en matière de défense et de sécurité*

L'obligation de continuité des activités judiciaires édictée par le code de la défense, la nécessité de développer la résilience des opérateurs d'importance vitale soulignée par le Livre blanc de la défense et de la sécurité nationale de 2013 constituent des objectifs structurels s'imposant à l'ensemble du dispositif de défense et de sécurité du secteur d'activités d'importance vitale.

L'approche suivie pour la construction et l'entretien des politiques de défense et de sécurité doit en conséquence prendre en compte la globalité des problématiques de sécurité. En effet, les liens cybernétiques et les interactions entre défense, sûreté, sécurité incendie, protection de la santé, sécurité des systèmes d'information sont tels qu'il convient de veiller avec la plus grande attention à s'affranchir des cloisonnements traditionnels entre métiers de la sécurité et à placer les impératifs de continuité des systèmes et de protection des personnes au cœur de la planification de défense et de sécurité.

### 4.1.1 Rationaliser les politiques de défense et de sécurité

Le PSO et le RSO déclinent un référentiel de défense et de sécurité permettant de rationaliser l'aménagement des établissements, en privilégiant la définition de niveaux d'équipement de sécurité. Chaque établissement fait par ailleurs l'objet d'une étude spécifique de sécurité, mettant en exergue ses contraintes particulières (configuration, mitoyenneté, zone exposée régulièrement au vandalisme ou aux mouvements sociaux, risques naturels, classement au titre du patrimoine…). Les projets immobiliers font l'objet d'une étude préalable de sécurité publique (voir 5.1.1).

### 4.1.2 Actualiser le cahier des charges pour les constructions d'établissements

A partir du RSO entretenu en temps réel par les opérateurs, il convient de compléter périodiquement le cahier des charges « défense et sécurité » correspondant à chaque type d'établissement nécessaire au fonctionnement de la justice.

## *4.2 Analyse et gestion des risques cybernetiques*

### 4.2.1 Adopter une démarche d'analyse et de gestion des risques

Au sein du SAIVAJ, tous les projets de modernisation comportant une dimension cybernétique mettant en œuvre des systèmes d'information doivent impérativement faire l'objet d'une analyse formalisée et d'une gestion rigoureuse des risques ; la dimension cybernétique peut résider dans l'utilisation de moyens électroniques pour préparer, suivre ou exécuter le projet (ex. : échange électronique de plans immobiliers entre le ministère et un prestataire, par courriel, sur cédérom ou tout autre support).

On appelle « système d'information » tout ensemble organisé de ressources (personnel, données, procédures, matériel, automates, caméra, autocommutateur, logiciel…) permettant d'acquérir, de stocker, de structurer et de communiquer des informations sous forme de textes, images, sons, ou de données codées dans des organisations.

L'analyse de risque d'un système d'information est un préalable indispensable à la définition de mesures de sécurité adaptées aux besoins. Les besoins de sécurité identifiés et la prise de risque résultant effectivement de la mise en œuvre du système sont ainsi clairement déterminés.

La méthode d'analyse de risque utilisée au sein du SAIVAJ est la méthode d'expression des besoins et d'identification des objectifs de sécurité (EBIOS). Créée en 1995 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et régulièrement mise à jour, cette méthode permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI).

L'utilisation de la méthode EBIOS comme méthode de référence favorise les échanges en matière d'analyse de sécurité tant au sein du ministère de la justice que vis-à-vis des partenaires extérieurs, aboutissant ainsi à bâtir un outil complet de gestion des risques SSI.

### 4.2.2 Conduire la démarche de gestion des risques, tout au long du cycle de vie d'un système d'information

Tout système traitant d'informations sensibles doit faire l'objet d'une analyse de risque, préalable indispensable à la définition de mesures de sécurité adaptées aux besoins. Les besoins de sécurité identifiés et la prise de risque résultant effectivement de la mise en œuvre du système sont ainsi clairement déterminés.

#### 4.2.2.1 Gestion des risques

La gestion des risques d'un système d'information est un processus itératif qui comprend les phases suivantes :

- l'appréciation du risque : cette tâche consiste à analyser et évaluer le risque ; cette phase se conclut par l'énoncé, par la maîtrise d'ouvrage, des objectifs de sécurité du système ;

- le traitement du risque : cette phase consiste à définir les mesures de sécurité (réduction, transfert ou prise de risque) applicables à la couverture des objectifs de sécurité énoncés à la phase précédente ;

- l'homologation de sécurité : la décision d'homologation est prise par l'autorité d'homologation, au vu du dossier d'homologation établissant que le système d'information considéré est apte à traiter des informations conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés. Le dossier comporte notamment :
  - la description fonctionnelle du système ;
  - l'analyse de risques ;
  - la politique de sécurité du système reprenant les référentiels de sécurité de l'information applicables au projet ;
  - les procédures d'exploitation de la sécurité ;
  - les conditions d'emploi qui s'imposent aux utilisateurs ;
  - l'analyse de la couverture des risques par les mesures ;

– le cas échéant, les agréments des dispositifs de sécurité.

Le dossier d'homologation est soumis à une commission constituée à cet effet présidée par le responsable central de la sécurité des systèmes d'information de l'OIV de l'autorité décisionnaire, réunissant les maîtrises d'ouvrage, les responsables de la sécurité des systèmes d'information de ces maîtrises d'ouvrage, la SDIT ainsi que le HFDS ; cette commission consulte en tant que de besoin des personnes qualifiées et mène toutes investigations nécessaires à la formulation de son avis sur l'homologation à l'autorité décisionnaire ;

- la décision d'homologation de sécurité est prononcée par l'autorité qualifiée en matière de défense et de sécurité définie à la ligne directrice n° 1. L'homologation de sécurité est prononcée pour une durée maximale de 5 ans mais doit être revue dès que le système d'information n'opère plus dans les conditions approuvées par l'autorité d'homologation ;

- la communication relative au risque vise à faire adhérer toutes les parties prenantes du système d'information à la gestion des risques, dans ses aspects humain, juridique, organisationnel et technique, par l'échange et le partage ;

- l'homologation de sécurité peut dans certaines situations faire l'objet de la compétence conjointe de plusieurs autorités qualifiées.

#### 4.2.2.2 Intégration de la SSI tout au long du cycle de vie des systèmes d'information

Dès les premières études réalisées en amont de tout projet de création ou d'évolution d'un système d'information, le DDS et le RSSI de chaque OIV sont consultés par la maîtrise d'ouvrage pour une prise en compte précoce des aspects sécurité de l'information. Le RSSI doit notamment rappeler à la maîtrise d'ouvrage l'obligation de constituer un dossier de sécurité (auquel est attribué un niveau entre 1 et 3) et de nommer un RSSI pour le projet.

##### *4.2.2.2.1 Détermination du niveau du dossier de sécurité*

La nature des enjeux de sécurité du projet (contexte, enjeux, interconnexion à d'autres SI *etc.*) permet de déterminer le niveau du dossier de sécurité qui est fixé par le DDS et le RSSI lorsque le système d'information reste interne à l'OIV ou par le HFDS dans les autres cas.

##### *4.2.2.2.2 Le dossier de sécurité de niveau 1*

Il comprend :
- les référentiels de sécurité de l'information applicables au projet ;
- une étude du contexte (enjeux, impacts, *etc*.) et l'identification des éléments essentiels (au sens EBIOS) ;
- une analyse formalisée des besoins de sécurité des éléments essentiels (informations et fonctions) traités par le SI.

##### *4.2.2.2.3 Le dossier de sécurité de niveau 2*

Il comprend :
– les référentiels de sécurité de l'information applicables au projet ;
– une analyse méthodique des risques, incluant l'étude du contexte et des enjeux, l'analyse formalisée des besoins de sécurité, l'analyse de la menace, et l'énoncé des objectifs de sécurité du système.

#### *4.2.2.2.4 Le dossier de sécurité de niveau 3 (appelé aussi dossier d'homologation)*

Il comprend :

– les référentiels de sécurité de l'information applicables au projet ;
– une analyse méthodique des risques, incluant l'étude du contexte et des enjeux, l'analyse formalisée des besoins de sécurité, l'analyse de la menace, et l'énoncé des objectifs de sécurité du système ;
– la validation formelle de la couverture des objectifs par les mesures de sécurité effectivement mises en œuvre, avec la reconnaissance explicite des risques résiduels.

#### *4.2.2.2.5 Liste des systèmes d'information dont le dossier de sécurité est de niveau 3*

Doivent disposer d'un dossier de sécurité de niveau 3 :

- tout système référencé dans la DNS comme élément essentiel d'un OIV ;
- tout système entrant dans le champ d'application du référentiel général de sécurité (RGS) ;
- tout système traitant d'informations classifiées, auquel s'appliquent en conséquence les règles interministérielles fixées par l'instruction générale interministérielle (IGI) n° 1300. En particulier, il convient de suivre la procédure d'homologation du système d'information au traitement d'informations classifiées.

Les systèmes d'information suivants, identifiés comme particulièrement sensibles au cours de l'analyse de risque préalable à la rédaction de la DNS, ont un dossier de sécurité de niveau 3 :

– le RPVJ (réseau privé virtuel du ministère de la justice) ;
– les centres de production informatique (Grigny et Nantes) ;
– l'application de gestion informatisée des PPSMJ ;
– les systèmes de placement sous surveillance électronique des PPSMJ ;
– l'application informatique de la chaîne pénale (Cassiopée) ;
– le système d'interceptions judiciaires ;
– le casier judiciaire ;
– le système d'information de la Chancellerie ;
– le système d'information du TGI de Paris ;
– le système AMALFI du livre foncier d'Alsace Moselle.

Cette liste est non exhaustive et d'autres systèmes d'information pourront être ajoutés par le HFDS.

### 4.2.2.3 Gestion de la documentation de sécurité

Le dossier de sécurité du système d'information doit être mis à jour par la maîtrise d'ouvrage à chaque évolution majeure du système (extension à des nouvelles fonctions ou informations, interconnexion à d'autres systèmes d'information), lorsque la réglementation change ou lorsque les conditions d'emploi évoluent (nouvelle menace, nouveau contexte, nouveaux enjeux, *etc*.)

Ces dossiers, dont la collection est tenue à jour par le HFDS, sont :

- protégés en confidentialité, disponibilité et intégrité ;
- dotés d'un numéro séquentiel de version et d'une date de mise à jour, ainsi que d'une page retraçant l'historique des modifications ;
- marqués d'une référence unique, permettant d'identifier clairement l'auteur, la date de création, des éléments de gestion de version ainsi que la mention de la classification du document, qui doit apparaître clairement sur le document.

#### 4.2.2.4 Recette et mise en exploitation du système d'information

La maîtrise d'ouvrage s'assure lors de la recette et de la mise en exploitation du système d'information de sa conformité aux exigences du dossier de sécurité.

- pour un dossier de sécurité de niveau 1 ou 2, elle valide par écrit cette conformité, en exprimant en tant que de besoin les réserves relatives à des points de non-conformité ;
- pour un dossier de niveau 3, la décision d'homologation relève de l'autorité qualifiée en matière de défense et de sécurité ;
- dans tous les cas, la validation mentionne explicitement les conditions d'emploi du système d'information.

#### 4.2.2.5 Fin de vie d'un SI ou de l'un de ses composants

Avant de procéder au retrait d'un système d'information ou de l'un de ses composants (mise hors service d'une application, ou d'un réseau, mise au rebut d'un matériel, changement d'organisation, *etc*.) la maîtrise d'ouvrage doit préalablement s'assurer que les besoins de sécurité des éléments essentiels évalués dans le dossier de sécurité demeurent pris en compte pendant et après l'opération de mise à l'arrêt.

A titre d'exemple :

- la confidentialité des informations devra être maintenue lors de la mise au rebut de supports ou de matériels ;
- la disponibilité et l'intégrité des informations ou des logiciels devront être assurées par un archivage approprié.

#### 4.2.2.6 Exigences minimales sur les produits de sécurité utilisés dans le SI

Afin de protéger un système d'information, il peut être nécessaire de mettre en place des produits de sécurité spécifiques : chiffreur, infrastructure de gestion de clefs, outils de signature électronique, système d'authentification, de contrôle d'accès, générateur de clefs cryptologiques, pare-feu, réseau privé virtuel sécurisé, outils de filtrage, systèmes d'horodatage, *etc*.).

Le dossier de sécurité doit mentionner explicitement les exigences d'assurance demandées par la maîtrise d'ouvrage ainsi que le niveau réel d'assurance du produit mis en place par la maîtrise d'œuvre.

Ces exigences d'assurance concernent principalement :

- la protection des données de configuration ou de paramétrage ;
- la validation et le filtrage éventuel des données en entrée avant tout traitement, qui concerne tant les saisies par des utilisateurs (risques d'erreur ou de tentative malveillante) que les données de provenance externe ; une attention particulière sera portée au contrôle des valeurs et aux limites ;
- la validation des données en sortie spécialement dans le cas d'une chaîne applicative. Une attention particulière sera portée au contrôle des valeurs et aux limites ;
- les risques de modification ou de corruption des données par l'applicatif lui-même ;
- la présence et la pertinence des mécanismes d'autocontrôle présents au sein de l'applicatif, et leur capacité à générer des notifications d'alerte lors de comportements anormaux ou simplement imprévus ;
- la présence et la pertinence de mécanismes de trace et de journalisation disponibles et configurables selon les besoins.

Les produits de sécurité mis en place doivent avoir fait l'objet d'une qualification de l'ANSSI au niveau requis par les objectifs de sécurité énoncés dans le dossier de sécurité du système d'information.

#### 4.2.2.7 Suivi du niveau de sécurité dans le temps

Un tableau de bord SSI est mis en place et tenu à jour. Il fournit au RCSSI et au HFDS une vision générale du niveau de sécurité et de son évolution dans le temps.

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

Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation des plans d'action.

# 5 LIGNE DIRECTRICE N° 3 : ORGANISER LA DÉFENSE ET LA SÉCURITÉ EN PROFONDEUR

## *5.1 Protection des sites et des personnes*

### 5.1.1 Études de sécurité publique

Une étude de sécurité publique, au sens des articles L114-1 à L114-4 et R114-1 à R114-3 du code de l'urbanisme, doit être réalisée préalablement à la délivrance de l'autorisation de construction ou d'aménagement pour toute opération de construction ou de réhabilitation afin d'identifier et de réduire, dès la conception, les vulnérabilités et les contraintes d'exploitation en matière de défense et de sécurité.

### 5.1.2 Périphérie des sites

Différentes zones de sécurité doivent être définies autour des établissements et des principes de circulation ou de stationnement des véhicules et d'accès des piétons au sein de ces zones doivent être clairement établis et formalisés au sein des plans particuliers de protection (PPP) des plans de protection (PP) et des plans de protection externe (PPE) en relation avec les autorités de police compétentes.

Les abords des sites d'importance vitale doivent si possible faire l'objet d'une surveillance vidéo avec capacité d'enregistrement (ces systèmes d'information entrant dans le périmètre de la ligne directrice n° 2), les ouvertures extérieures doivent être protégées, et des dispositifs physiques interdire l'entrée en force des véhicules.

L'attention des autorités administratives compétentes devra systématiquement être appelée sur les contraintes de sécurité devant être prises en compte pour la mise en œuvre des politiques d'urbanisme, et de la police de la circulation, du stationnement, et des autres activités prenant place sur le domaine public.

### 5.1.3 Découpage interne des sites en zones de sécurité

#### 5.1.3.1 Types de zones de sécurité

Chaque établissement du SAIVAJ est découpé en 4 types de zones de sécurité :

- zone publique (pour l'accueil du public par exemple) ;
- Zone publique sécurisée (pour les personnes justifiant d'un titre ou d'une convocation)
- zone administrative (bureaux du ministère par exemple) ;
- zone restreinte (par exemple une salle serveurs, une salle des scellés, une armurerie, *etc*.) ;
- zone de détention.

Chaque PSO prévoit le découpage de ses établissements en zones de sécurité, définit les règles de contrôle d'accès à ces zones ainsi que les règles organisant le passage entre les zones, en respectant la règle selon laquelle il est interdit de passer d'une zone non administrative à une autre sans passer par une zone administrative. Les dérogations concernant les bâtiments anciens, dans lesquels l'application de ces règles présenterait des difficultés insurmontables, doivent être accompagnées de mesures compensatoires.

Dans une zone administrative ou restreinte, tout visiteur ou justiciable doit être pris en charge à l'entrée de la zone, puis accompagné tout au long de sa visite et raccompagné à la fin jusqu'à la sortie de la zone sous la responsabilité de la personne à qui il rend visite. De manière générale, tout personnel de la zone visitée a un devoir de vigilance sur la circulation et les comportements des visiteurs, tant pour ce qui concerne la sécurité des personnels et des biens que vis à vis du patrimoine informationnel (support informatique ou même support papier).

### 5.1.3.2 Zonage spécifique aux espaces judiciaires

#### *5.1.3.2.1 La zone publique*

La zone publique comprend les espaces du palais de justice destinés à accueillir le public (justiciables, visiteurs, avocat,…). Les horaires d'ouverture et fermeture ainsi que les modalités concernant les audiences tardives et les audiences tenues le week-end doivent être définis.
Le poste de contrôle du public situé à l'entrée du bâtiment constitue un passage obligé pour accéder à cette zone.
La zone publique comprend :

- le poste central de contrôle du public ;
- l'accueil ou le service d'accueil unique du greffe ;
- la salle des pas perdus ;
- les salles d'audience…

#### *5.1.3.2.2 La zone publique sécurisée*

La zone publique sécurisée est l'espace public de la juridiction uniquement accessible aux personnes justifiant d'un titre ou d'une convocation. Elle regroupe les bureaux des magistrats et fonctionnaires destinés à accueillir du public. Afin d'assurer la protection des personnes, les bureaux situés dans cette zone recevant du public font l'objet d'une sécurisation particulière.
L'accès à cette zone est limité :

- au personnel ;
- aux justiciables munis d'une convocation ;
- aux prestataires appelés à y pénétrer dans l'excercice de leurs fonctions munis également d'un titre d'accès ;
- aux visiteurs pris en charge et accompagnés par le personnel.

#### *5.1.3.2.3 La zone administrative*

La zone administrative comprend l'espace du palais réservé au personnel et excluant tout public. Elle regroupe les bureaux des magistrats et fonctionnaires qui ne sont pas destinés à recevoir du public, ainsi que les parties communes telles que la cafétéria ou salle de convivialité, la bibliothèque, le parking, le local courrier. L'accès à la zone administrative se fait via la zone publique ou la zone publique sécurisée ou directement depuis l'extérieur du palais de justice.

#### *5.1.3.2.4 La zone restreinte*

La zone restreinte comprend l'espace du palais dont l'accès est limité uniquement à quelques personnes habilitées à y pénétrer dans l'exercice de leur fonction. Cette zone comprend notamment :

- le poste de contrôle sécurité sûreté ;
- le local des pièces à conviction : espace réservé au stockage des objets placés sous scellés, situé en zone restreinte. Son accès ainsi que la détention des clés sont réservés uniquement aux membres du personnel affectés à ce service ainsi qu'au greffier en chef du service. La gestion des pièces à conviction requiert une vigilance accrue.
- le local des archives ;

– le local de reprographie ;

Les équipements de contrôle d'accès mis en place sont identiques à ceux de la zone administrative. Leur paramétrage sera toutefois différent puisque l'accès à la zone restreinte est limité à quelques membres du personnel.

#### *5.1.3.2.5 La zone détenus*

La zone détenus correspond à l'espace du palais réservé aux détenus avant leur comparution. Cette zone fait l'objet d'une attention particulière et d'équipements spécifiques en matière de sûreté : poste sûreté dédié, cellules, sas pour les fourgons cellulaires, couloirs de circulation étanches. Elle comprend notamment :

– Le dépôt, les cellules ou l'attente gardée ; les cellules sont les pièces dans lesquelles sont isolés les détenus en attendant d'être jugés. Les attentes gardées sont des lieux (salles, couloirs…) situés à proximité immédiate des salles d'audience ou des cabinets des juges, destinés à accueillir, généralement pour une très courte durée, les détenus avant leur comparution devant un juge.

– Le sas fourgon ; le sas fourgon est un accès sécurisé permettant l'entrée du fourgon dans la juridiction. Il s'agit d'un passage clos, muni de deux systèmes de fermeture dont on ne peut ouvrir l'un que si l'autre est fermé. Une fois dans le sas fourgon, le détenu peut sortir du véhicule sous escorte, afin de rejoindre les cellules d'attente gardées ou le dépôt avant d'être conduit vers les box des salles d'audiences en utilisant les accès qui lui sont dédiés.

– Les couloirs de circulation des détenus : la séparation physique des flux de population évite les situations de rencontre entre personnes pouvant donner lieu à des incidents. Ainsi, les détenus escortés ne doivent pas avoir de contact avec le personnel judiciaire ou le public, voire parfois avec d'autres détenus depuis l'arrivée du fourgon jusqu'au box de la salle d'audience.

#### *5.1.3.2.6 Le box sécurisé des salles d'audience*

Les box sécurisés en salles d'audiences sont des espaces fermés destinés à accueillir les prévenus retenus sous escorte. Deux types de sécurisation du box détenus sont recommandés : le premier à vitrage complet du box, le second à barreaudage en façade avec un vitrage sur les faces latérales côté public et coté magistrats.

### 5.1.3.3 La video-protection au sein des juridictions

La vidéo protection peut être définie comme une application de techniques de création et d'exploitation d'images à distance. Elle consiste à installer des caméras de surveillance dans un lieu public ou privé en vue de prévenir tout acte de malveillance (intrusion, vol…).

Elle permet d'exploiter a posteriori des images pour identifier des auteurs d'actes de malveillance et facilite l'opération de « levée de doute » la nuit par des sociétés de télésurveillance, sous réserve qu'il soit satisfait aux exigences de la politique ministérielle de sécurité des systèmes d'information dont relève la vidéo protection.

Il conviendra de prévoir un dispositif de vidéo protection couplé à des détecteurs d'alerte anti-intrusion dans les locaux suivants :

– l'entrée principale ;
– les diverses entrée utilisées ;
– les locaux des scellés ;

– le sas fourgon ;
– tous les circuits sécurisés ;

Il conviendra de prévoir un dispositif de vidéo protection seul pour les locaux suivants :

– les parkings situés autour du bâtiment ;
– la salle des pas perdus ;
– diverses circulations telles que celles menant aux services de l'instruction et des mineurs ;
– les façades ;
– les principaux couloirs de circulation, notamment ceux menant aux services sensibles et aux locaux des scellés ;
– certaines façades sensibles.

La vidéo protection doit être proscrite dans les salles d'audiences et ne doit pas filmer les postes de travail dans les zones non publiques du palais.

### 5.1.3.4 Le personnel en charge de la sûreté au sein des services judiciaires

La sûreté des sites judiciaires dépend également de la présence du personnel en charge de la sûreté. Les juridictions définiront le dispositif à mettre en place en fonction des personnels disponibles (viviers de réservistes et de retraités) et des contraintes budgétaires.

#### *5.1.3.4.1 Les forces de l'ordre*

– en application du protocole Justice-Intérieur du 6 janvier 2011, elles restent en charge de la sécurisation des audiences de comparution immédiate, des sessions de cours d'assises et des procès signalés sensibles en termes d'ordre public ;
– en cas de situation de crise affectant une juridiction, les forces de l'ordre peuvent être amenées à intervenir en application des plans de protection externes (PPE) dont l'élaboration et la mise en œuvre relèvent des préfets.

#### *5.1.3.4.2 Les personnels retraités*

– les retraités de l'administration pénitentiaire : ces agents ont exercé durant leur carrière la fonction de surveillant, de premier surveillant ou de chef de service pénitentiaire. Ils sont employés en qualité de contractuels et ne peuvent effectuer que 720 heures annuelles (soit 18 heures par semaine réparties sur 10 mois). Ils exercent des missions de contrôle d'accès/filtrage des juridictions et de surveillance des sites.
– la réserve civile pénitentiaire : sous l'autorité du chef de greffe de la juridiction (ce dernier mettant en œuvre les mesures de sûreté définies par les chefs de cours), le titulaire du poste est chargé du contrôle des accès et de la surveillance générale des locaux relevant du palais de justice, dans le souci d'assurer la protection des personnes et des biens. La loi pénitentiaire n° 2009-1436 du 24 novembre 2009 porte création de la réserve civile pénitentiaire. Un contrat d'engagement est signé entre le réserviste et l'employeur (SAR). Ces agents volontaires retraités, issus des corps de l'administration pénitentiaire peuvent rejoindre la réserve civile dans la limite de cinq ans à compter de la fin de leur lien avec le service. Les réservistes peuvent effectuer jusqu'à 150 vacations annuelles de 7 heures. Ils sont mis à disposition par la direction interrégionale des services pénitentiaires du ressort dans lequel est situé le domicile du réserviste.
– les réservistes de la police et de la gendarmerie nationale : ils exercent des missions de contrôle d'accès/filtrage des juridictions et des missions de police d'audience sous forme de patrouilles dynamiques. Le protocole national signé conjointement le 6 janvier 2011 par le ministère de la justice et le ministère de l'intérieur a défini l'organisation de ces missions.

- il est à préciser que, si les réservistes continuent de relever de l'autorité hiérarchique des DDSP ou des commandants de groupement de gendarmerie, ils restent soumis fonctionnellement à l'autorité des chefs de juridiction. Les réservistes de la police nationale peuvent effectuer jusqu'à 150 vacations de 7 heures par an. Les réservistes militaires de la gendarmerie nationale peuvent effectuer pour le compte des services judiciaires 30 vacations par an
- les agents de sociétés privées de sécurité : ils sont employés en juridiction sur la base de contrats de droit privé par des sociétés retenues dans le cadre de marchés publics. Leurs formations les conduisent à assurer exclusivement des missions de contrôle d'accès/filtrage, aux côtés de missions de sécurité incendie requérant une qualification SSIAP selon la règlementation en vigueur concernant les établissements recevant du public (ERP). Il convient d'ailleurs de préciser que la présence sur site des agents de sécurité incendie, lorsqu'elle est requise dans les ERP les plus importants, se limite aux horaires d'ouverture au public.

#### 5.1.3.5 Câblages réseaux et informatiques

- Chaque OIV est responsable de la protection physique des équipements et des ressources réseau. Les règles de protection doivent respecter les contraintes suivantes :
- un câblage réseau reliant deux équipements situés en zone restreinte ne peut transiter par une zone administrative ;
- les locaux hébergeant des autocommutateurs, des serveurs ou des équipements réseau ou télécom doivent se trouver dans une zone restreinte ;
- les règles d'accès physique et logique aux postes de travail ou équipements situés hors d'une zone administrative doivent être renforcées par rapport à celles relatives à l'accès aux postes situés dans une zone administrative.Lorsqu'elle est située dans une zone publique ou dans une zone de détention, une prise réseau ne peut être brassée que si elle est en permanence connectée à un équipement identifié du SAIVAJ. Les services offerts par cet équipement doivent être limités et contrôlés. De plus, l'accès physique à la prise réseau doit être protégé pour interdire à d'autres équipements de s'y connecter.

- Dans une zone administrative ou restreinte, une prise réseau brassée ne peut être mise à disposition (dans une salle de réunion par exemple) sans formalisation des règles de connexion, de contrôle de l'accès physique à la salle, de contrôle de l'accès physique à la prise, et de limitation et de contrôle des services offerts par la connexion à cette prise.

- Les panneaux de raccordement et les salles des câbles doivent être placés en dehors des zones d'accueil du public, et leur accès doit être contrôlé.

- Sur les systèmes d'information particulièrement sensibles, les procédures d'exploitation de la sécurité intègrent des contrôles anti-piégeage réguliers effectués par du personnel formé ; il peut être fait appel à des services spécialisés (opérations dites de dépoussiérage).

### 5.1.4 Postes d'inspection et de filtrage

- Les établissements pénitentiaires, les points d'importance vitale, les principaux établissements recevant du public mettent systématiquement en œuvre une capacité d'inspection et de filtrage de tous les flux entrées/sorties permettant de s'assurer physiquement de l'absence de substances explosives ou inflammables, d'armes ou d'objets dangereux ou interdits portés par la personne elle-même, ou contenus dans son bagage.

- Au sein des PIV, une traçabilité des accès par les visiteurs externes aux zones restreintes doit être mise en place. ces traces doivent être conservées un an, conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Hors les établissements pénitentiaires, une procédure dérogatoire d'entrée peut être instaurée au bénéfice de personnes titulaires d'un badge d'entrée, dûment identifiées et enregistrées à chacun de leur passage, préalablement signataires d'une charte d'usage et inscrites dans un cercle de confiance duquel elles peuvent être exclues en cas de manquement aux règles de sécurité.

Les personnes bénéficiaires de cette procédure dérogatoire sont néanmoins soumises au respect des mesures physiques de contrôle organisées de manière aléatoire à l'initiative de l'autorité fonctionnelle de l'établissement, ou en application des consignes prises en application du plan VIGIPIRATE.

- Le dispositif de contrôle d'accès physique doit s'appuyer sur des produits qualifiés par l'ANSSI et bénéficier d'un maintien en condition opérationnelle rigoureux quand il comporte tout ou partie des fonctionnalités suivantes :
  - authentifier, autoriser et enregistrer l'accès à une ressource physique (contrôle d'accès) ;
  - détecter, alerter et enregistrer toute tentative d'accès non autorisé (détection d'intrusion) ;
  - assurer les activités de vidéosurveillance (VS) fournissant au personnel de sûreté un système de caméras disposées sur l'ensemble du site, de transport des flux vidéo, d'enregistrement, d'archivage et de visionnage de ces vidéos ;
  - superviser et gérer l'ensemble des équipements et bâtiments du site, et disposer d'une vue globale des équipements de sécurité de ces bâtiments.

### 5.1.5 Demande de présentation d'une pièce d'identité

Les contrôles, vérifications et relevés d'identité, au sens des articles 78-1 à 78-6 du code de procédure pénale, relèvent de la seule compétence des officiers de police judiciaire et, sous certaines réserves, des agents de police judiciaire et des agents de police judiciaire adjoints.

Toutefois, les chefs des établissements ont compétence pour prendre « *les mesures nécessaires pour assurer la sécurité* » des personnes qui travaillent dans l'établissement, sur le fondement de l'article L. 230-2 du code du travail, applicable aux agents publics en vertu de l'article 3 du décret n° 82-453 du 28 mai 1982 relatif à l'hygiène et à la sécurité du travail ainsi qu'à la prévention médicale dans la fonction publique.

Sur ce fondement, les chefs d'établissement peuvent, si les circonstances l'exigent, décider que chaque personne souhaitant pénétrer dans les locaux de l'établissement présente un document d'identité à l'agent affecté à l'accueil du public. Il ne peut s'agir que d'une mesure d'ordre intérieur visant à assurer la sécurité des locaux et, en aucune façon, d'un contrôle d'identité ou d'un relevé d'identité au sens des dispositions du code de procédure pénale.

En cas de refus ou d'impossibilité pour la personne de justifier de son identité, l'accès aux locaux peut être refusé ; en revanche, aucune autre mesure ne peut être envisagée.

### 5.1.6 Accès aux juridictions

On dénombre cinq types d'accès au palais de justice :

- accès du public ;
- accès piéton du personnel ;
- accès au SAS fourgon ;
- accès véhicule destiné au parking du personnel ;
- accès des véhicules de livraison ;

D'une manière générale :

- éviter les croisements entre les différentes catégories de personnes ;
- concilier l'exigence de fluidité des accès par des contrôles différenciés en fonction de la qualité des personnes (personnel, public, auxiliaires de justice, détenus…).
- verrouiller les accès et organiser des circuits de flux ;

- L'accès du public

- la procédure d'accès du public définit des horaires d'ouverture et de fermeture ainsi que des modalités dans le cas des audiences tenues le week-end (ouvertes au public) ;
- la juridiction ne devra, de préférence, disposer que d'un accès public ;
- surveiller cet accès ainsi que son abord extérieur immédiat (rondes aléatoires ou visionnage en continu, à l'aide d'un équipement de vidéosurveillance relié au PCS) ;
- filtrer l'entrée ;
- afficher les horaires du public ;

- L'accès piéton du personnel (zone administrative) : prévoir des modalités d'accès propre à chaque population :

- le personnel emprunte l'accès piéton afin de se rendre directement dans son service ou éventuellement dispose d'un accès propre à partir du parking qui lui est réservé. Il dispose alors d'une clé, d'un badge ou d'un digicode ;
- le public ne peut accéder à la juridiction par cet accès et doit se présenter à l'accès unique du public;

- L'accès au dépôt et/ou attente gardée :

- surveiller l'arrivée du fourgon à l'aide d'un équipement de vidéo protection relié au PCS du dépôt dans les situations courantes ;
- interrompre la circulation sur la voirie aux abords des bâtiments judiciaires lors des procès sensibles ;
- renforcer la présence des forces de l'ordre.

- L'accès des véhicules du personnel

- prévoir un accès filtré réservé au personnel grâce à un portail automatique commandé par badge par exemple.

- L'accès des véhicules de livraison

- l'immatriculation du véhicule des prestataires extérieurs, le nom du chauffeur ainsi que la copie d'un document justifiant de son identité doivent être demandés par la personne ayant passé commande (pièces remises au service ou à la personne chargée de réceptionner la livraison qui vérifiera la concordance des informations). Les livraisons devront être programmées.

- Accès des prestataires extérieurs :

- les entrées réservées aux livraisons sont indépendantes de celles du public et du personnel.
- l'immatriculation du véhicule des prestataires extérieurs, le nom du chauffeur ainsi que la copie d'un document justifiant de son identité doivent être demandés par la personne ayant passé commande (pièces remises au service ou à la personne chargée de réceptionner la livraison qui vérifiera la concordance des informations) ;
- détection par passage d'un miroir sous les véhicules (véhicules de service, de livraison ou de fonction) en période Vigipirate, ou dans les sites sensibles ;
- tout changement fait l'objet d'un avis à la personne ayant passé la commande ;
- accompagnement du livreur par un agent du site est obligatoire s'il est amené, dans l'exercice de ses fonctions, à entrer à l'intérieur de la juridiction ;

Au niveau de la juridiction :

- délivrer carte ou badge d'accès (annuels ou temporaires), ou laissez-passer ; actualiser ces moyens d'accès à chaque changement de personnel ;
- établir une liste journalière d'émargement des personnels d'entreprise présents sur le site ;
- établir un organigramme des clés, comprenant avec l'organisation d'une gestion des clés, l'identification des personnes ou des entreprises qui possèdent des clés ou des passes :
- limiter strictement le nombre de personnes détentrices de clés ou de passes (agents du PCS et mainteneurs) ;
- mettre en place un outil de suivi des clés avec mention de leur restitution.
- produire un casier judiciaire (B3) des personnels intervenant sur le site et éventuellement mener une enquête de moralité préalable (ceci est valable uniquement pour les entreprises présentes en permanence sur le site comme le gardiennage, le ménage ou la maintenance) ;

Au niveau de l'entreprise

- obligation de communiquer, par l'entreprise, la liste des personnels habilités à intervenir sur le site judiciaire, avec en annexe la copie des pièces d'identité ;
- obligation de remise d'un planning délimitant la durée de l'intervention et précisant le service ou la zone concernée, par les entreprises intervenant ponctuellement ;
- obligation de communiquer la liste des personnels effectuant des remplacements (48 heures à l'avance).

### 5.1.7 Portiques de détection

En cas d'installation d'un portique de sécurité, il convient d'affecter à l'accueil un ou plusieurs agents présentant les aptitudes nécessaires, afin que l'utilisation de cet appareil ait lieu dans les meilleures conditions.
Un magnétomètre peut être utilisé si la juridiction ne possède pas de portique détecteur de métaux ou en complément, au portique pour localiser sur l'individu l'emplacement de l'objet qui a déclenché l'alarme.
L'obligation faite à toute personne relevant ou ne relevant pas du cercle de confiance (voir 5.1.4), y compris les auxiliaires de justice, d'emprunter un portique de détection pour pénétrer dans la juridiction, ne porte pas, par elle-même, atteinte au libre exercice des droits de la défense (CE, 21 octobre 1988, Syndicat des avocats de France).

### 5.1.8 Contrôle des bagages à main, des effets personnels, des livraisons

Il ne peut être procédé à aucune fouille à corps ni fouille des bagages à main qui sont assimilées par la jurisprudence de la Cour de cassation à des perquisitions ne pouvant être effectuées que sous les conditions et dans les formes prévues par le code de procédure pénale.

En revanche, l'inspection visuelle des bagages à main est possible, notamment au moyen d'un système de détection à rayons X ; les agents affectés au contrôle peuvent demander à ce que les visiteurs ouvrent leurs sacs pour permettre d'en voir le contenu. Les objets tranchants ou inhabituels (ex : cutters, couteaux, tournevis, *etc.*) peuvent être consignés pour être rendus aux intéressés à leur sortie de l'établissement à condition qu'une mention soit portée sur un registre tenu au poste d'inspection-filtrage.

Si la personne refuse de se plier à cette exigence, l'accès aux locaux de l'établissement peut lui être refusé.

### 5.1.9 Systèmes de ventilation et de traitement d'air

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne doivent être élaborées, portées à la connaissance du personnel et vérifiées annuellement.

En fonction de la sensibilité des établissements, des mesures de protection seront mises en œuvre visant à garantir la non accessibilité des systèmes de ventilation.

### 5.1.10 Systèmes d'alimentation et de distribution d'énergie

L'alimentation secteur des équipements devra être conforme aux réglementations applicables de façon à se prémunir des atteintes à la sécurité des personnes et des équipements pouvant découler d'un défaut électrique.
En fonction de la sensibilité des établissements, des mesures de contrôle d'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie seront mises en œuvre.

### 5.1.11 Planification locale de défense et de sécurité

Le PPP ou le PP, ainsi que le PPE comportent un plan d'action centré sur la sécurité des audiences et des autres activités judiciaires mobilisant tant le concours des agents de sécurité du ministère de la justice que les forces publiques présentes dans l'enceinte judiciaire ou appelées en renfort.

Le dispositif à mettre en œuvre doit permettre une détection et une caractérisation précoces des actes redoutés, le repérage de signaux faibles faisant présager une évolution non prévue de la situation, l'alerte rapide des forces publiques et l'adoption immédiate d'une posture d'alerte au sein de l'établissement ; il fait l'objet d'une graduation en fonction de la sensibilité prévisible des audiences et des activités judiciaires programmées.

### 5.1.12 Protocole d'intervention avec les forces publiques et les secours

Le dispositif d'action relatif à la sécurité des audiences et des autres activités judiciaires doit si possible faire l'objet d'un cadre concerté d'intervention pour garantir une action adaptée et réactive des forces de l'ordre et des secours sur alerte qualifiée. Ce protocole sera intégré au PPP ou PP et au PPE.

### 5.1.13 Campagnes de sensibilisation du personnel

Il convient d'organiser périodiquement des sessions d'information destinées aux différentes catégories de personnels portant sur les risques encourus et les moyens de protection et de prévention mis à leur disposition.

### 5.1.14 Prévention des comportements violents

Dans des services les plus exposés aux comportements violents, des mesures doivent être mises en place pour minimiser les risques d'exposition des personnels :
– programmes de prévention de la violence ;

- dispositifs de traçabilité favorisant une meilleure transparence des conditions de fonctionnement du service ;
- dispositif d'écoute et de soutien des personnels en cas d'événement de sécurité ;
- veille active pour détecter les situations dangereuses ;
- dispositions particulières à intégrer le cas échéant au sein des planifications locales de défense et de sécurité.

#### 5.1.15 Dispositif d'alerte au sein des services judiciaires : le dispositif EMMA

« EMMA », pour EMission de Message d'Alerte, est un dispositif informatique individuel d'alerte dont les fonctionnalités permettent aux magistrats et fonctionnaires de disposer en juridiction, sur leur ordinateur, d'une capacité d'alerte silencieuse en cas de difficulté.
Son objectif est de rompre l'isolement en permettant aux agents en difficulté de lancer une alerte silencieuse chaque fois qu'ils s'estiment en difficulté ; cet équipement vient en complétement des dispositifs existants (portiques de sécurité, vidéo protection, systèmes anti-intrusion) ou pallient leur absence, en particulier dans les tribunaux d'instance.

## *5.2 Protection des infrastructures d'information et de communication*

### 5.2.1 Notion de défense en profondeur

La protection des infrastructures d'information et de communication reposait encore récemment sur le concept de protection périphérique. Or, la mise en place d'un moyen de protection unique, aussi sophistiqué soit-il, fait prendre un risque inacceptable car, en cas de défaillance, c'est l'ensemble du système qui se trouve exposé.

Au contraire, l'adoption d'une démarche de défense en profondeur permet de constituer plusieurs lignes de défense composées de différents moyens. Cependant, afin que le dispositif mis en œuvre atteigne une performance supérieure à celle procurée par une simple juxtaposition, sa disposition doit respecter certaines règles d'architecture :

- indépendance des lignes de défense : la compromission d'un moyen ne doit pas fournir à l'attaquant un avantage pour en compromettre un autre (pas de possibilité d'effet dit château de cartes) ;
- coordination des actions : la défense ne peut pas être isolée ; elle doit envisager le problème posé de manière globale et organiser la coordination des actions dans ce cadre global ;
- complétude des moyens : chaque ligne de défense doit être constituée de moyens (des barrières) permettant de faire face à toutes les menaces retenues.

### 5.2.2 Gestion des biens

Toute protection des infrastructures d'information et de communication nécessite préalablement la connaissance précise de la consistance de ces infrastructures et des informations contenues.

#### 5.2.2.1 Cartographie des systèmes d'information

Chaque établissement établit et maintient à jour un inventaire des ressources informatiques placées sous sa responsabilité, en s'appuyant sur un outillage adapté :

- cet inventaire comprend la listes des briques matérielles et logicielles utilisées, ainsi que leurs versions exactes ;
- il est constitué d'une base de données de configurations maintenue à jour ;
- l'historique des attributions des biens inventoriés doit être conservé dans le respect de la législation ;
- la cartographie précise les centres informatiques, les architectures des réseaux, pour lesquels sont identifiés les points névralgiques et la sensibilité des informations manipulées, et qualifie le niveau de sécurité attendu ;
- ces inventaires et cartographies sont tenus à disposition du RSSI et de la cellule d'appui du HFDS.

#### 5.2.2.2 Qualification et protection de l'information

La sensibilité et la protection de toute information doivent être évaluées, conformément aux dispositions de la ligne directrice n° 4.

### 5.2.3 Protection du réseau de transport de données

Les réseaux de transport de données du SAIVAJ doivent disposer de certaines garanties de fonctionnement en temps de crise ainsi que d'une robustesse suffisante pour faire face à la cybercriminalité :

- tout équipement au sein du ministère de la justice réalisant un point d'interconnexion physique ou logique entre un réseau intérieur au RPVJ et un réseau extérieur à ce périmètre, qu'il soit public ou privé, doit être installé, géré, administré et utilisé sous la responsabilité de la SDIT ;
- cette règle s'impose pour tout système d'information du ministère (serveurs, postes de travail, téléphones, copieurs multifonctions, machines à affranchir, systèmes de signalétique, *etc*.)

#### 5.2.3.1 Règles de protection physique des réseaux de transport

De manière générale, les chemins de câbles et les locaux de répartition doivent bénéficier des règles de protection physique mentionnées dans la présente ligne directrice.
L'accès physique aux locaux techniques doit être restreint aux seules personnes ayant à intervenir matériellement et dont la liste est tenue à jour.
Les plans doivent faire l'objet de mesures techniques et organisationnelles limitant leur divulgation non autorisée.
Les prises non utilisées doivent être retirées.

#### 5.2.3.2 Sécurisation des réseaux nationaux

Le ministère de la justice utilise les infrastructures nationales (ADER puis RIE) en respectant les règles de sécurité qui leur sont rattachées :

- seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'un établissement : il est interdit de brancher des moyens informatiques personnels sur le réseau du ministère (voir également 9.2.3) ;
- toute interconnexion entre les réseaux locaux d'un établissement et un réseau externe doit être réalisée via les infrastructures nationales. Une connexion par un dispositif physique ou logique non fourni par la SDIT est strictement interdite ;
- les connexions des machines du réseau interne vers l'extérieur doivent être filtrées ;
- les accès à Internet passent obligatoirement par les passerelles nationales.

#### 5.2.3.3 Sécurisation des réseaux locaux

Le ministère de la justice doit assurer la maîtrise des interconnexions et configurer de manière adéquate les équipements des réseaux actifs :

- le système d'information doit être segmenté en zones présentant un niveau homogène de sécurité ;
- l'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet et de passerelles sécurisées et validées par le HFDS ;
- dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place ; si le cloisonnement n'est pas physique, les mesures prises doivent être validées par les HFDS concernés ;
- des équipements filtrants doivent être mis en place entre le réseau de transport et chaque site disposant d'un serveur ;
- pour permettre le paramétrage des équipements de contrôle de flux et de filtrage, la SDIT fournit aux opérateurs le plan d'adressage à implémenter sur les sites, et procède régulièrement au contrôle de la conformité de l'adressage réel au plan prévu.

#### 5.2.3.4 Sécurisation des réseaux sans fil

- tout déploiement de réseau sans fil doit faire l'objet d'une analyse de risque spécifique ;
- les protections intrinsèques étant insuffisantes, des mesures complémentaires validées par le HFDS doivent être mises en œuvre dans le cadre de la défense en profondeur ;
- une segmentation du réseau doit être mise place pour limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio ;
- à défaut de mise en œuvre de mesures spécifiques validées, le déploiement de réseaux sans fil sur des systèmes d'information manipulant des données sensibles est interdit.

#### 5.2.3.5 Cas particulier des réseaux téléphoniques

Les systèmes de téléphonie constituent des systèmes d'information. Ils englobent des autocommutateurs (PABX, IPBX), des réseaux, des terminaux, fixes et mobiles et véhiculent de la voix, éventuellement en audioconférence, et parfois des visioconférences :

- les logiciels de téléphonie sur les postes de travail suivent les règles de gestion et d'utilisation des logiciels relevant des services informatiques. Les flux réseaux doivent être filtrés en cohérence avec ces règles d'utilisation ;
- le numéro d'appelant présenté à l'appelé n'offrant aucune garantie d'authenticité, il ne peut servir de base pour identifier l'interlocuteur, par exemple pour l'accès à un service ou à une boîte vocale ;
- l'usage de la VoIP impose l'usage de VLAN dédiés ;
- les autocommutateurs doivent bénéficier des règles de protection physique mentionnées au 5.6.3 ; l'accès physique doit être restreint aux seules personnes ayant à intervenir matériellement et dont la liste est tenue à jour ;
- les postes d'administration et d'exploitation bénéficient de la même protection.

#### 5.2.3.6 Cas particulier des réseaux support des systèmes industriels

On entend par systèmes industriels les systèmes composés de capteurs/actionneurs et de calculateurs ayant pour finalité de surveiller, contrôler ou commander des installations techniques. A ce titre on identifie notamment :

- la gestion technique de bâtiment (GTB) ayant pour finalité de surveiller, contrôler ou commander des installations techniques de bâtiments (distribution électrique, éclairage, ventilation, climatisation, *etc*.) ;

- le contrôle d'accès physique et la surveillance qui ont pour objet de surveiller ou de contrôler l'accès à un lieu, un bâtiment, un local ou des équipements spécifiques ;
- les systèmes de sûreté ou systèmes instrumentés de sécurité (SIS) ayant pour finalité de protéger les biens et les personnes en cas d'incendie ou autre sinistre susceptible d'affecter une installation ;
- les systèmes industriels métier, systèmes spécifiques à une activité donnée, comme par exemple les systèmes de supervision de processus métier (SCADA).

Ces réseaux doivent profiter d'un cloisonnement physique (qui peut être commun entre eux) à l'égard des réseaux supportant les flux métiers ou bureautiques. A défaut, des mesures complémentaires validées par le HFDS doivent être prises.
La tierce maintenance applicative sur ces réseaux ne peut être envisagée qu'à travers des outils qualifiés par l'ANSSI.

#### 5.2.3.7 Réalisation et tenue à jour de la cartographie réseau

L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture et des configurations maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des SI.

#### 5.2.3.8 Filtrage élémentaire

L'opérateur met en place un blocage préventif des connexions à Internet pouvant provoquer directement ou indirectement des dysfonctionnements ou mettre en danger le réseau de transport de données, telles que :
- les connexions à des ressources fortement consommatrices de bande passante (vidéo, audio, *etc*.) ;
- les connexions vers des sites susceptibles de propager des virus, de mettre en œuvre un contrôle à distance ou de récupérer des informations sur les ordinateurs connectés au réseau ;
- les connexions à des ressources dont l'accès peut porter atteinte à la réputation de l'institution judiciaire (pornographie, contrefaçon de logiciels, *etc*.) ;
- les connexions qui, par l'identification du ministère comme source de la connexion, pourraient provoquer des réactions hostiles (infection, déni de service, déstabilisation par voie de presse) ou conduire à des réponses trompeuses.

Le cas échéant, des accès dédiés ou banalisés, sans raccordement au réseau de transport de données du SAVAIJ, doivent être mis en place.

#### 5.2.3.9 Sécurisation des accès spécifiques

Le ministère de la justice s'assure que les accès spécifiques à Internet nécessitant des droits particuliers - pouvant porter atteinte à la sécurité du SI - pour un usage métier ne peuvent être mis en place qu'après dérogation dûment justifiée, sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation.

### 5.2.4 Formalisation des procédures et des règles d'exploitation sécurisées des systèmes d'information

#### 5.2.4.1 Documentation et procédures

Pour chaque système d'information, la maîtrise d'ouvrage est responsable du dossier de sécurité ainsi que de la documentation de sécurité qui y est intégrée, et permet d'assurer le maintien opérationnel du système.
La maîtrise d'ouvrage demande à la maîtrise d'œuvre d'établir et de tenir à jour la convention de service, le journal d'exploitation, et les procédures d'exploitation et de la sécurité adaptées au système (PES).
L'ensemble des documents constitutifs des dossiers de sécurité sont centralisés par les RCSSI. Les PES, validées par la cellule du HFDS, seront mises en ligne et accessibles aux utilisateurs et aux acteurs concernés par la mise en œuvre du système, en particulier par les administrateurs.

#### *5.2.4.1.1 La convention de service*

Elle formalise l'organisation et les responsabilités respectives de la maîtrise d'ouvrage et de la maîtrise d'œuvre en matière d'exploitation du SI. Ce document doit comporter les informations suivantes :
- liste des procédures d'exploitation (alerte et gestion des incidents de sécurité, application des correctifs de sécurité, sauvegardes, plan de continuité, *etc*.) ;
- liste des responsabilités associées à chacune de ces procédures ;
- points de contact pour les opérations d'exploitation du SI ;
- liste des personnes possédant les droits administrateurs sur le SI ;
- liste des évolutions et mises à jour majeures (matérielles ou logicielles) du SI.

La convention de service doit être approuvée par la maîtrise d'ouvrage et la maîtrise d'œuvre.

#### *5.2.4.1.2 Le journal d'exploitation*

Celui-ci consigne au jour le jour de manière précise et explicite les opérations d'exploitation et les événements observés sur le SI. Ce journal d'exploitation est à usage interne à la maîtrise d'œuvre, mais la maîtrise d'ouvrage peut à tout moment en obtenir la consultation.

#### *5.2.4.1.3 Les procédures d'exploitation de la sécurité adaptées au système (PES)*

Les PES doivent, au minimum, définir la gestion des incidents de sécurité, comprenant la continuité d'activité, ainsi que la remonté d'alertes.

### 5.2.4.2 Journalisation

La journalisation des systèmes et réseaux revêt une importance fondamentale. Elle permet d'opérer une détection des anomalies qui peuvent être définies et répertoriées a priori (exemples : scrutation de ports, rejet d'authentification, flux coupé par un pare-feu), de qualifier ces anomalies en incidents et de prévoir une réaction appropriée dans les délais les plus courts en optimisant la méthode de transmission de l'alerte, ses destinataires, la nature de la réaction, *etc*.

#### *5.2.4.2.1 La journalisation*

La journalisation système et réseau consiste en l'observation, la mesure, la collecte et la conservation des traces à l'aide d'outils appropriés ; elle constitue une tâche permanente des équipes techniques de production et d'exploitation d'un système d'information. Cette journalisation doit se faire sur :
- les serveurs applicatifs ;
- les serveurs d'infrastructure système ;
- les serveurs d'infrastructure réseau ;
- les équipements de sécurité ;
- les postes d'ingénierie et de maintenance, pour les systèmes industriels ;
- les équipements réseau ;
- les postes d'administration.

La gestion des traces de sécurité est définie dans le guide détaillé des procédures et règles d'exploitation du système d'information qui doit comprendre :

- la collecte sécurisée des traces de sécurité ;
- la protection des traces contre tout effacement, altération ou accès non autorisé ;
- le contrôle de l'intégrité des mécanismes de traces ;
- le filtrage et analyse des traces ;
- l'archivage des traces ;
- l'effacement des fichiers des traces obsolètes (obsolescence et durée d'archivage doivent être fixées) ;
- la destruction des traces selon le délai légal ou déclaré.

#### *5.2.4.2.2 La détection*

- l'opérateur met en œuvre un système de corrélation et d'analyse de journaux qui exploite les événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité des systèmes d'information.
- ce système de corrélation et d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection d'événements susceptibles d'affecter la sécurité des systèmes d'information.
- l'opérateur installe et exploite ce système de corrélation et d'analyse de journaux conformément aux règles de l'art.

#### *5.2.4.2.3 La réaction*

- l'opérateur, tient à jour, avec les maîtrises d'ouvrage et met en œuvre les procédures de traitement d'incidents de sécurité affectant le fonctionnement ou la sécurité des systèmes d'information qu'il exploite.
- l'opérateur procède au traitement des incidents de sécurité conformément aux règles de l'art en matière de réponse aux incidents de sécurité.
- en particulier, l'opérateur met en place un système d'information spécifique pour traiter les incidents et stocker et analyser les relevés techniques. Ce système est cloisonné vis-à-vis des systèmes concernés par l'incident.
- lorsque l'opérateur fait appel à un prestataire pour le traitement des incidents, le prestataire doit être qualifié par l'autorité nationale en matière de sécurité de système d'information.
- l'opérateur conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'au moins six mois.
- l'opérateur tient ces relevés techniques à la disposition de la cellule d'appui du haut fonctionnaire de défense et de sécurité.

#### *5.2.4.2.4 Journalisation applicative*

- les journaux doivent être protégés en intégrité et en disponibilité et leur accès limité aux seuls intervenants autorisés. Il est nécessaire d'horodater de manière cohérente les événements de sources multiples afin de permettre une corrélation fiable des journaux.
- l'objectif de la journalisation applicative est de permettre l'imputation a posteriori d'opérations effectuées par des utilisateurs d'une application ; elle nécessite que soient assurées la collecte et la conservation des traces de ces opérations.
- les traces constituées ne sont jamais exploitées de manière systématique, mais uniquement en cas de besoin et sur réquisition formelle de l'autorité habilitée.

- la définition et la mise en œuvre de la journalisation applicative devront tenir compte des contraintes législatives et réglementaires relatives au traitement des informations nominatives (loi n° 78-17 du 6 janvier 1979 relative à l'informatique, aux fichiers et aux libertés).
- la procédure d'exploitation des traces est définie précisément au niveau de chaque système d'information. Lorsque la maîtrise d'œuvre du système d'information n'est pas assurée par l'OIV, l'autorité hiérarchique désirant mettre en œuvre cette procédure en formule la demande par écrit au HFDS qui la transmet à la maîtrise d'œuvre après s'être assuré de sa validité.

#### 5.2.4.3 Règles strictes encadrant les interventions des prestataires sur les systèmes d'information

Le recours aux prestations de service, dès lors que la sécurité d'un système d'information représente un enjeu majeur pour le SAIVAJ, ne doit pas dériver vers une sous-traitance de la gestion de l'exploitation. Les menaces directes induites par ce type de recours nécessitent la mise en œuvre des règles suivantes :

##### *5.2.4.3.1 Clauses de sécurité*

Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité présentes dans les cahiers des charges et les contrats qui spécifient :

- les responsabilités et les procédures qui doivent être établies entre l'organisme et les prestataires afin de permettre l'imputabilité d'éventuels incidents ;
- les mesures SSI que le prestataire doit respecter dans le cadre de ses activités (ces clauses ne peuvent être moins strictes que celles définies).

Dans ce cadre, une attention renforcée sera portée sur la gestion des droits et habilitations accordés à ces prestataires (des audits fréquents doivent être programmés).
Le RCSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

##### *5.2.4.3.2 Suivi et contrôle des prestations fournies*

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

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

##### *5.2.4.3.3 Hébergement*

L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf dérogation dûment motivée et précisée dans la décision d'homologation, ou accord du HFDS.
Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI : mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, *etc*.).

##### *5.2.4.3.4 Intégration des clauses SSI dans les contrats de sous-traitance de développement informatique*

Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :

- formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;

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

#### 5.2.4.4 Gestion des incidents

Ce chapitre précise la manière dont est effectué le partage de l'information (alertes, incidents) de façon à lutter efficacement contre les attaques. Il ne se substitue pas au chapitre 7.2.

##### *5.2.4.4.1 Chaînes opérationnelles SSI*

Les chaînes opérationnelles des ministères concourent à l'effort national de cyber sécurité ; la coordination des compétences est organisée à l'échelon ministériel selon le schéma d'organisation précisé au 7.2.
En cas d'alerte de sécurité identifiée au niveau national, le FSSI, les RCSSI et l'ensemble de la chaîne fonctionnelle SSI du ministère, sollicités par l'organisation de gestion de crise, s'assurent de la bonne application des exigences formulées par les instances nationales dans les meilleurs délais.

##### *5.2.4.4.2 Traitement des incidents*

La chaîne fonctionnelle SSI est informée par la chaîne opérationnelle de tout incident de sécurité et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.
Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI d'une entité ou d'un ministère, fait l'objet d'un compte-rendu par le FSSI, via la chaîne SSI, au centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

## *5.3 Responsabilisation et sensibilisation des utilisateurs des systèmes d'information*

### 5.3.1 Définir des règles cohérentes d'authentification et de contrôle d'accès

Dans le cas général, l'accès d'un utilisateur à un système d'information et l'attribution de certains droits s'effectuent après une phase d'identification (déclinaison de l'identité) et d'authentification (preuve de l'identité).

#### 5.3.1.1 Identification

L'identification se fait par présentation d'un identifiant (*login*) ; l'identifiant est une donnée publique non révocable par l'utilisateur. Cette identification peut être renforcée par la présentation et vérification d'une donnée biométrique (elle aussi publique non révocable). L'identification doit établir un lien non équivoque entre l'identifiant et l'utilisateur.

La traçabilité des opérations et le diagnostic des anomalies de sécurité imposent une identification non équivoque du propriétaire d'un accès. Lors de la phase d'identification préalable à l'accès à un système d'information, l'identifiant se rapporte donc toujours à un seul individu et non à une entité générique (groupe d'utilisateurs).

Les PSO doivent expressément prévoir les cas où l'organisation du travail rendrait l'application de cette règle difficile (permanence, contraintes opérationnelles). Dans ces cas dûment justifiés, l'identification logique des utilisateurs peut être générique, mais elle doit être complétée par un dispositif d'identification physique non équivoque.

#### 5.3.1.2 Authentification

L'authentification simple se fait par mot de passe (donnée secrète et révocable par l'utilisateur) ; l'authentification peut être renforcée par la présentation d'un objet matériel contenant une donnée secrète et révocable par l'utilisateur : carte à puce, jeton USB, *etc*.
Le renforcement de l'authentification logique par la présentation d'un objet matériel dédié est appelé authentification forte.
L'objectif à atteindre en matière de mise en place de protocoles d'authentification sur les systèmes d'information du SAIVAJ est le suivant : l'interaction entre un utilisateur et un système d'information ne peut se produire sans une authentification préalable forte, mutuelle et réciproque entre cet utilisateur et le système d'information.

#### 5.3.1.3 Mots de passe

Un mot de passe est une donnée secrète choisie par l'utilisateur et lui seul. Il peut être modifié par l'utilisateur à tout moment. Comme son utilisation engage le titulaire, il ne doit pas être révélé ou donné à quiconque (même à un supérieur hiérarchique ou un administrateur informatique) sous aucun prétexte et même à titre temporaire (les actions illicites doivent demeurer imputables) :

- les mots de passe ne doivent jamais être conservés en clair sur un système d'information ;
- les administrateurs informatiques ne doivent jamais connaître les mots de passe des utilisateurs. Cependant, ils doivent être capables de les changer sur décision de l'autorité hiérarchique ou sur demande de l'utilisateur ;

Si pour des raisons impérieuses de service (urgence avérée, ou indisponibilité majeure de l'utilisateur ou de l'administrateur), l'accès à un SI doit se faire sous l'identité d'un utilisateur indisponible, la seule procédure autorisée est la suivante :

- les utilisateurs inscrivent leur mot de passe sur un papier placé dans une enveloppe cachetée et identifiée à leur nom ;
- les enveloppes sont remises à l'autorité hiérarchique qui les place en sûreté dans une armoire forte ;
- en cas de besoin impérieux, le supérieur hiérarchique ou son représentant ouvre l'enveloppe ;
- jusqu'au retour de l'utilisateur indisponible, l'utilisation du compte se fait sous la responsabilité de l'autorité hiérarchique qui a ouvert l'enveloppe.

#### 5.3.1.4 Caractéristiques obligatoires du mot de passe

- la durée maximale entre deux renouvellements est fixée par l'OIV. Cette durée ne peut être supérieure à 6 mois ;
- un mot de passe doit avoir une longueur minimum de 8 caractères ;
- il doit comporter au minimum 1 minuscule, 1 majuscule, 1 chiffre et 1 caractère spécial ;
- lors de la création d'un mot de passe, un outil doit vérifier le respect des règles et la qualité du mot de passe ;
- lors d'un renouvellement obligatoire, le nouveau mot de passe doit être différent du précédent ;
- aucun mot de passe, ni secret (clef de chiffrement, clef privée d'authentification ou de signature) ne doit résider en clair, sur aucun fichier au sein du SI.

#### 5.3.1.5 Contrôle d'accès

- pour chaque système d'information, la maîtrise d'ouvrage définit les profils d'utilisateur du SI (ces profils sont parfois appelés rôles) en ce qui concerne les besoins en droits d'accès ;
- la définition des profils et des droits associés doit se conformer au 6.1.3.3 ;
- conformément à son profil, l'utilisateur aura exclusivement accès aux ressources et aux informations dont il a besoin dans l'accomplissement de sa tâche ;
- des profils particuliers seront prévus pour les personnels de sociétés prestataires de service opérant sur le SI ;
- la protection de l'intégrité des tables contenant les privilèges doit faire l'objet d'un contrôle particulier par la maîtrise d'ouvrage du système d'information ;
- la définition des profils devra prendre en compte les dispositifs planifiés de gestion des situations d'exception (absence de personnels qualifiés, vacance de poste, congés, reprise d'activité, *etc.*) et de gestion des incidents.

#### 5.3.1.6 Verrouillage des sessions de travail

Les postes de travail sont les points d'entrée principaux du système d'information. Les utilisateurs doivent être sensibilisés à rendre leur environnement de travail inaccessible en leur absence (verrouillage de la session, arrêt du poste de travail).

Pour renforcer cette mesure et éviter des négligences, une mesure de verrouillage automatique des sessions de travail après un délai d'inactivité est mise en place sur le réseau de transport de données de l'opérateur ; cette mesure se traduit par l'apparition d'un écran de veille lorsque le poste de travail n'est pas utilisé pendant dix minutes. L'utilisateur doit entrer son mot de passe pour ouvrir à nouveau la session de travail.

### 5.3.2 Cohérence des règles

La cohérence des règles d'authentification et de contrôle d'accès aux systèmes d'information et de communication doit être recherchée pour l'ensemble des systèmes nécessitant un même niveau de

protection ainsi que pour les systèmes destinés aux mêmes personnels. Ces règles doivent comprendre en particulier :

- les mécanismes d'authentification ;
- la gestion des mots de passe ;
- la gestion des comptes et des identités (nominatifs ou fonctionnels) ;
- les moyens de recouvrement ;
- le contrôle d'accès ;
- le cloisonnement des réseaux ;
- la maîtrise des flux ;
- la télé-administration et la télémaintenance ;
- la suppression des accès non maîtrisés au système d'information ;
- l'attribution des privilèges, y compris le contrôle des privilèges attribués ;
- la protection des postes de travail ;
- les contraintes particulières liées à la mobilité et au nomadisme ;
- l'utilisation de matériels ou de logiciels personnels.

### 5.3.3 Utilisation du matériel, nomadisme

#### 5.3.3.1 Inventaire des matériels et des logiciels du système d'information de l'OIV

Les services responsables de l'achat et de l'installation de matériels ou de logiciels informatiques doivent tenir à jour l'inventaire de ces matériels et logiciels. Cet inventaire participe au processus de cartographie des systèmes d'information :

- en tant que matériels, sont compris les postes fixes, les postes portables, les périphériques (imprimantes, photocopieuses réseau, scanners, *etc*.), les téléphones portables, les assistants personnels (PDA), ainsi que les supports amovibles (clefs USB, disques durs externes, *etc*.) ;
- cet inventaire comporte notamment l'identité de l'agent ou du service auquel le matériel ou le logiciel a été attribué. L'inventaire est tenu à jour jusqu'à la mise au rebut du matériel ou du logiciel ;
- la SDIT fournit les outils de gestion d'inventaire.

#### 5.3.3.2 Postes de travail et règles de protection

Tous les postes de travail, y compris les postes nomades, sont administrés par les services informatiques du SAIVAJ. En tant qu'éléments des systèmes d'information, leur administration doit se faire conformément à une procédure d'exploitation de la sécurité spécifique. Celle-ci doit prendre en compte les points liés à l'exploitation des systèmes d'information et ceux liés à la sécurisation des moyens de l'utilisateur.
Les terminaux fixes recouvrent également les télécopieurs : ces derniers ne doivent pas être connectés au RPVJ.

#### 5.3.3.3 Gestion et utilisation des supports amovibles

Les supports amovibles (clef USB, disque dur externe, *etc*.) fournis par un opérateur du SAIVAJ à ses agents doivent être inscrits à l'inventaire des matériels informatiques. Le cas des DVD ou CD-ROM réinscriptibles sera traité au sein de chaque OIV.
Tout support amovible fourni par les services informatiques et affecté à un utilisateur doit au préalable avoir subi un formatage bas niveau. Il en sera de même lorsque le support amovible est réaffecté à un autre utilisateur ou un autre usage.

Les supports amovibles qui ne sont pas fournis professionnellement sont interdits à la connexion sur un poste de travail, sauf exception prévue par le PSO. C'est le cas en particulier des périphériques ayant des capacités de stockage et/ou de calcul : ordiphones, téléphones mobiles, appareils et cadres photographiques numériques, baladeurs MP3, *etc*.
La connexion d'un support amovible du SAIVAJ à un équipement extérieur est interdite. Par exemple, il est interdit de connecter une clef USB professionnelle sur un équipement domestique.
Avant la connexion d'un support amovible ou l'insertion d'un CDROM ou DVD, l'utilisateur doit s'assurer que le poste de travail dispose d'un anti-virus actif, dont la base de signatures est à jour.
Tout fichier ouvert ou transféré à partir d'un support amovible vers un poste SAIVAJ est systématiquement analysé par l'anti-virus du poste SAIVAJ.
Tout fichier dont la confidentialité est de niveau 2 ou 3 (voir ligne directrice n° 4) doit être chiffré avant son transfert vers un support amovible. L'outil de chiffrement doit être adapté et autorisé par le RSSI.

#### 5.3.3.4 Téléphonie et règles de protection des terminaux mobiles professionnels

Les téléphones à combiné sans fil (DECT, *bluetooth* ou autres technologies) émettent des signaux compromettants (voir 6.3.5) propices aux interceptions illégales et doivent être évités. Leur utilisation est interdite pour le traitement des informations classifiées et très vivement déconseillée pour les informations sensibles.
Les principes de protection des terminaux mobiles sont identiques à ceux des postes de travail informatiques dès lors que les matériels en permettent l'application :
- authentification de l'utilisateur par mot de passe (PIN) renouvelé régulièrement ;
- blocage lors d'échecs d'authentification successifs (trois échecs par défaut) ;
- verrouillage automatique en cas d'inactivité ;
- mise à jour des logiciels le cas échéant, en particulier sur les ordiphones ;
- désactivation des fonctions inutiles ou inutilisées ;
- désactivation des interfaces non filaires inutiles (*Wi-Fi*, *bluetooth*, infrarouge) ;
- utilisation d'un mot de passe pour l'accès à la messagerie vocale ;
- chiffrement des données stockées ;
- surveillance constante (vol possible) ;
- extinction et conservation dans un endroit sûr si la surveillance ne peut être continue ;
- prudence lors de la réception de minimessages (*SMS*), lesquels peuvent contenir des liens vers des sites web malveillants, susceptibles d'infecter les ordiphones ;
- procédure de réaction en cas de perte ou de vol, en relation avec le service gestionnaire et l'opérateur.

La discrétion des conversations est de mise en particulier lors de l'utilisation d'un téléphone mobile ou d'un ordiphone dans un lieu public.

#### 5.3.3.5 Sécurisation des copieurs multifonctions

Pour disposer d'un niveau de sécurité homogène, il est nécessaire de sécuriser l'ensemble des matériels sur le réseau, y compris les imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions doivent être paramétrés de façon à :
- exclure leurs capacités à communiquer avec l'extérieur du RPVJ ;
- garantir le contrôle de l'utilisateur, du déclenchement d'une impression de données à caractère sensibles (utilisateur authentifié sur son poste) jusqu'à la récupération du support imprimé (utilisation d'un code utilisateur sur l'imprimante/copieur multifonctions).

## 5.4 Formation et sensibilisation aux problématiques de défense et de sécurité

Les plans de formation et de sensibilisation sont la condition d'une bonne appropriation des politiques et des règles de défense et de sécurité par les personnels du SAIVAJ. Une sensibilisation régulière vise à maintenir une vigilance constante.
A l'échelle du SAIVAJ et au sein de chaque OIV, un plan de formation et de sensibilisation à la défense et à la sécurité doit être prévu au bénéfice des agents chargés de missions de défense et de sécurité ou constituant des relais naturels auprès de l'ensemble des utilisateurs, afin de favoriser une bonne appropriation des règles de défense et de sécurité fixées au niveau du SAIVAJ et des opérateurs.
Toute maîtrise d'ouvrage doit systématiquement prévoir un volet SSI au sein des formations à l'utilisation des applications métiers qu'elle met en place ; ce volet portera notamment sur la conduite du changement des comportements en matière de sécurité ; il aura notamment pour objectif de renforcer l'efficacité du réseau d'alerte SSI.

## 5.5 Éléments à prendre en compte dans la rédaction des procédures d'exploitation de la sécurité (PES)

Lors de la réalisation du dossier de sécurité, les PES nécessaires à l'exploitation du système sont rédigées dans le respect des prescriptions de l'analyse de risque et du socle commun de mesures techniques décrit ci-après. Quand une mesure ne peut être totalement appliquée, il convient de faire le nécessaire pour être le plus conforme possible à la mesure et de justifier de l'écart dans les documents d'exploitation ainsi que dans le dossier de sécurité de l'application.

### 5.5.1 Sécurité des réseaux - sécurisation des mécanismes de commutation et de routage

Afin d'être protégés des attaques, les mécanismes de commutation et de routage doivent être ainsi configurés :

- protocoles de couches basses : une attention particulière doit être portée à leur implantation afin d'être protégés des attaques usuelles par saturation ou empoisonnement de cache (exemple : le protocole ARP) ;
- routage dynamique : la mise en place de protocoles de routage dynamique, lorsqu'elle est nécessaire, doit être accompagnée d'une surveillance des annonces de routage et de procédures permettant de réagir rapidement en cas d'incidents ; e protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY ;
- session EGP : lors de sa mise en place avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY ;
- mots de passe par défaut : ils doivent impérativement être modifiés, de même que les certificats ;
- durcissement des équipements réseaux (comme les routeurs) : ils doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et des

certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

### 5.5.2 Exploitation des systèmes d'information

#### 5.5.2.1 Sécurité des ressources informatiques

La surveillance et la configuration des ressources informatiques constituent le socle de leur sécurité. Il est donc nécessaire de durcir les configurations et de surveiller les interventions opérées sur celles-ci. Il est impératif de documenter et mettre en œuvre :

- la traçabilité des interventions sur le système : les interventions de maintenance sur les ressources informatiques de l'entité doivent être répertoriées par le service informatique et être accessibles au correspondant SSI local durant au moins un an ;
- la configuration des ressources informatiques et leur maintien à jour : les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur dans l'entité ou, par défaut, en vigueur au niveau central ;
- le suivi et la mise à jour de la documentation des configurations : la configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

#### 5.5.2.2 Autorisations et contrôles d'accès

Les procédures doivent spécifier :

- l'identification, l'authentification et le contrôle d'accès logique :

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

- les droits d'accès aux ressources :

- après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes du besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès) et de moindre privilège (chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission) ;

- la gestion des profils d'accès aux applications :

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

- les autorisations d'accès des utilisateurs :

- toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel ;

- la revue des autorisations d'accès :

- une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du correspondant local SSI ;

– l’application de cette procédure doit être un indicateur du tableau de bord des RCSSI ;

- la confidentialité des informations d’authentification :

– les informations d’authentification (mots de passe d’accès aux SI, clés privées liées aux certificats électroniques, *etc*.) doivent être considérées comme des données sensibles (voir la ligne directrice n° 4 de la PMDS) ;

- la gestion des mots de passe :

– les mots de passe ne doivent pas être stockés en clair (par exemple dans un fichier) sur les postes de travail et ne doivent en aucun cas transiter en clair sur les réseaux ;

- l’initialisation des mots de passe :

– chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique ;

- la politique des mots de passe :

– les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, doivent être conformes aux règles édictées par la PMDS ;

- l’utilisation de certificats électroniques qui doit respecter les règles du RGS ;
- le contrôle systématique de la qualité des mots de passe :

– des moyens techniques permettant d’imposer la politique de mots de passe (par exemple pour s’assurer du respect de l’obligation relative à l’usage de caractères spéciaux) doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé ;

- le séquestre des authentifiants « administrateur » :

– les authentifiants permettant l’administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L’authentifié doit être informé de l’existence de ces opérations de gestion, de leurs finalités et limites ;
– tout accès d’administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit ;
– les informations d’authentification bénéficiant d’un moyen de protection physique (notamment une carte à puce) n’ont, par défaut, pas besoin d’être l’objet d’opérations de séquestre de la part d’autres personnels que l’authentifié lui-même ;

- la politique particulière aux mots de passe « administrateur » :

– chaque administrateur doit disposer d’un mot de passe propre et destiné à l’administration ;

- la gestion du départ d’un administrateur des SI :

– en cas de départ d’un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d’administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l’administrateur).

#### 5.5.2.3 Sécurisation de l’exploitation

Une liste minimale de procédures à mettre en œuvre pour assurer la sécurité de l’exploitation doit être précisée :

- la restriction des droits :

- sauf exception dûment motivée et validée par la chaîne fonctionnelle SSI, les utilisateurs n'ont pas de droits d'administration ;

    - la protection des accès aux outils d'administration :

- l'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès (tracée et auditable) ;

    - l'habilitation des administrateurs :

- l'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation ;

    - la gestion des actions d'administration :

- les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration ;

    - la sécurisation des flux d'administration :

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

    - la centralisation de la gestion du système d'information :

- afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser autant que possible des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information ;

    - la sécurisation des outils de prise de main à distance :

- la prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents habilités par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre ;
- des mesures de sécurité spécifiques (journalisation des opérations, audits réguliers, *etc*.) doivent être définies et respectées pour sécuriser cet usage ;

    - la définition d'une politique de gestion des comptes du domaine :

- une politique explicite de gestion des comptes du domaine doit être documentée ;

    - la configuration de la stratégie des mots de passe des domaines :

- la politique de gestion des mots de passe doit être conçue de façon à se protéger contre les attaques par essais successifs de mots de passe. La complexité dans le choix des mots de passe doit être conforme à la PMDS (voir 5.3.1.4.) ;

    - la définition et l'application d'une nomenclature des comptes du domaine :

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

    - la restriction au maximum de l'appartenance aux groupes d'administration du domaine :

– l’appartenance aux groupes du domaine « administrateurs de l’entreprise » et « administrateurs du domaine » n’étant nécessaire que dans de très rares cas, leur attribution doit se faire sur justification ;
– les opérations les plus courantes doivent être effectuées avec des comptes du domaine « membres des groupes locaux d’administration » des ordinateurs ou ayant une délégation d’administration ;

- les comptes de service :

– les comptes de service ont la particularité d’avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation. Le recensement de ces comptes doit faire l’objet d’une procédure auditable et être assorti d’un contrôle régulier ;
– ces comptes doivent faire l’objet d’une restriction des droits, en suivant le principe du moindre privilège ;

- la désactivation des comptes obsolètes du domaine :

– il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, qu’il s’agisse de comptes d’utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine ;

- l’amélioration de la gestion des comptes d’administrateurs locaux :

– afin d’empêcher la réutilisation des empreintes d’un compte utilisateur local d’une machine à une autre, il convient soit d’utiliser des mots de passe différents pour les comptes locaux d’administration, soit d’interdire la connexion à distance via ces comptes ;

- la maintenance externe :

– les données non chiffrées doivent être effacées avant l’envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés par l’ANSSI. L’effacement des données sensibles doit s’appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec le HFDS ;

- la mise au rebut :

– lorsqu’une ressource informatique est amenée à quitter définitivement l’entité, 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, ou respecter des procédures établies en concertation avec le HFDS ;

- la protection contre les codes malveillants :

– des logiciels de protection contre les codes malveillants (les anti-virus) doivent être installés sur l’ensemble des serveurs d’interconnexion, serveurs applicatifs et postes de travail de l’entité ;
– ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé ;

- la gestion des événements de sécurité de l’antivirus :

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

- la mise à jour de la base de signatures :

– les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par la sous-direction de l'informatique et des télécommunications ;

- La configuration du navigateur internet :

– le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès internet ou intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, *etc*.)[4] ;

- la définition et la mise en œuvre d'une politique de suivi et d'application des correctifs de sécurité :

– le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être documenté et adapté, dans sa mise en œuvre, suivant les contraintes et le niveau d'exposition du système ;

- le déploiement des correctifs de sécurité :

– les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par la sous-direction de l'informatique et des télécommunications ;

- la migration des systèmes obsolètes :

– les logiciels utilisés sur le système d'information doivent relever d'une version pour laquelle l'éditeur assure le support, et doivent être tenus à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de préciser les mesures adaptées qui seront prises ;

- l'isolation des systèmes obsolètes restants :

– il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable ;
– cette isolation doit être documentée et, chaque fois que cela est possible, doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI) ;

- la journalisation des alertes :

– chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être structurées de manière à permettre leur corrélation avec l'ensemble des autres traces du SI et être conservées de manière sûre ;

- la définition et la mise en œuvre d'une politique de gestion et d'analyse des journaux de traces :

– une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI de la SDIT, validée par le HFDS, puis mise en œuvre ;

- la conservation des journaux :

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

[4] Voir par exemple sur le site ssi.gouv.fr la note n° DAT-NT-16/ANSSI/SDE/NP du 2 avril 2014 : recommandations pour le déploiement sécurisé du navigateur *Google Chrome* sous *Windows*.

#### 5.5.2.4 Exploitation sécurisée des centres informatiques

Les responsables de l'exploitation des centres informatiques doivent s'assurer pour chacun des points ci-dessous que les règles minimales présentées sont bien documentées et mises en œuvre :

- systèmes d'exploitation :

– les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service ;
– seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque ;
– une attention particulière doit être apportée aux comptes administrateurs ;

- applications dites n-tiers :

Elles doivent, pour être mises en œuvre, répondre aux prérequis suivants :
– logiciels déployés pour le tiers présentation : la mise en œuvre d'une configuration renforcée est obligatoire (ex : serveur Web, Reverse Proxy) et sera décrite dans le dossier d'architecture technique (DAT) puis validée par le RSSI ;
– logiciels en tiers application : des règles de développement sécurisé (voir « sécurité du développement des systèmes ») et les configurations des logiciels en tiers application doivent être spécifiées et appliquées. Elles sont détaillées dans le cadre de cohérence technique (CCT) ;
– logiciels en tiers données : des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données. Ces règles doivent être détaillées dans le cadre de cohérence technique (CCT) ;

- passerelle d'échange de fichiers :

– les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS, *etc*.). Toute dérogation doit faire l'objet d'une justification validée par le RSSI ;

- messagerie technique :

– pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone d'arrière guichet (*back-office*) du centre informatique. Cette messagerie technique ne doit être en aucun cas utilisée directement par un utilisateur ;

- filtrage des flux applicatifs :

– de façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre ;
– les équipes d'exploitation tiennent à jour une matrice de gestion des flux applicatifs permettant l'audit des configurations des équipements opérant ce cloisonnement ;

- flux d'administration de deux types :

– flux d'administration de l'infrastructure (réservés aux agents du centre informatique) ;
– flux d'administration des applications métier (réservés à la direction métier) ;

L'attribution des droits d'administration doit respecter cette différenciation et les deux types doivent être, dans la mesure du possible, cloisonnés physiquement par l'utilisation d'un réseau de gestion d'infrastructure dédié ;

- service de noms de domaine – DNS technique :

– dans le cas du déploiement d'un serveur de noms de domaine pour les besoins techniques internes au centre informatique, on utilisera les extensions sécurisées DNSSEC ;

- effacement de support :

– le reconditionnement et la réutilisation des disques durs pour un autre usage (exemple : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisée des données (avec un produit certifié par l'ANSSI) ;

- destruction de support :

– la fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur, *etc*.) doit s'accompagner d'une opération de destruction des supports de stockage avant remise au constructeur ;

- traçabilité / imputabilité :

– afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP ou *network time protocol*) qu'ils spécifient dans la documentation (DAT, dossier d'exploitation, *etc*.) ;

- supervision :

– un cloisonnement logique entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place et documenté ;

- accès aux périphériques amovibles :

– l'accès aux supports informatiques amovibles fait l'objet d'un traitement adapté, plus particulièrement lorsque ces supports ont été utilisés pour mémoriser de l'information sensible ou pour conduire des opérations d'exploitation ;

- accès aux réseaux :

– le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, *etc*.) doivent être documentés ;

- audit/contrôle :

– un planning d'audits est défini et piloté par le RSSI du système d'information relevant de sa responsabilité. Ces audits peuvent être diligentés par le HFDS ;
– tous résultats d'audit ainsi que les plans d'actions qui en découlent doivent être portés à la connaissance du HFDS.

## *5.6 Sécurisation des moyens de l'utilisateur*

### 5.6.1 Sécurisation des postes de travail

Le durcissement des configurations des postes de travail est une condition nécessaire à la sécurité des utilisateurs et du système d'information. Il convient de définir une procédure d'exploitation de la sécurité prenant en compte l'ensemble des points ci-dessous et de s'assurer de sa mise en œuvre sur le périmètre sur lequel elle s'applique.

- fourniture et gestion des postes de travail :

– les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par la sous-direction de l'informatique et des télécommunications ;

- formalisation de la configuration des postes de travail :

– la procédure formalisée de configuration des postes de travail est établie par chaque direction, conformément aux directives de la PMDS ;

- verrouillage de l’unité centrale des postes fixes :

– lorsque l’unité centrale d’un poste fixe est peu volumineuse, donc susceptible d’être facilement emportée, elle doit être protégée contre le vol par un système d’attache (par exemple un câble antivol) ;

- verrouillage des postes portables :

– un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation ;

- réaffectation du poste de travail :

– la procédure définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés ;

- privilèges des utilisateurs sur les postes de travail :

– la gestion des privilèges des utilisateurs sur leur poste de travail doit suivre le principe du moindre privilège : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission ;
– l’attribution de ces droits doit se faire à la prise de poste ;
– le processus de suppression des droits au départ de l’utilisateur doit être documenté ;

- utilisation des privilèges d’accès « administrateur » :

– les privilèges d’accès « administrateur » doivent être utilisés uniquement pour les actions d’administration le nécessitant ;

- gestion du compte « administrateur local » :

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

- stockage des informations :

– dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des directions et en accord avec les règles de sécurité en vigueur ;

- sauvegarde / synchronisation des données locales :

– dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs avec leur documentation ;

- partage de fichiers :

– le partage de répertoires ou de données hébergées localement sur les postes de travail est strictement interdit ;

- suppression des données sur les postes partagés :

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

- chiffrement des données sensibles :

– une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs (avec sa documentation) afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles ;

- fourniture de supports de stockage amovibles :

– les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par l'équipe locale chargée des SI. L'usage de supports de stockage amovibles personnels est à proscrire ;

- accès à distance aux systèmes d'information de l'entité :

– les accès à distance aux SI de l'entité (accès dits nomades) doivent être réalisés via les infrastructures nationales. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est obligatoire ;

- pare-feu local :

– un pare-feu local conforme aux directives de la PMDS doit être installé sur les postes nomades ;

- stockage local d'informations sur les postes nomades :

– le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé ;

- 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 ;

- désactivation des interfaces de connexion sans fil :

– des règles de configuration des interfaces de connexion sans fil (*Wi-Fi*, *bluetooth*, 3G, *etc.*), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin ;

- configuration des interfaces de connexion sans fil :

– elle doit être établie de façon à interdire les usages dangereux de ces interfaces ;

- utiliser des outils de vérification automatique de la conformité :

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

### 5.6.2 Sécurisation des copieurs multifonctions

Les paramètres des imprimantes et copieurs multifonctions doivent faire l'objet d'une grande attention afin de diminuer leur surface d'attaque. Elles ne doivent pas pouvoir communiquer avec l'extérieur.

- le traitement des impressions des informations sensibles :

Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression (utilisateur authentifié sur son poste) jusqu'à la récupération du support imprimé (utilisation d'un code utilisateur sur l'imprimante).

### 5.6.3 Sécurisation de la téléphonie

Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes est une obligation. Une procédure d'exploitation de la sécurité relative à la téléphonie doit au minimum prendre en compte :

- la sécurisation de la configuration des autocommutateurs :

Les autocommutateurs doivent être maintenus à jour *via* l'installation des correctifs de sécurité. Leur configuration doit être durcie. En particulier il faut s'assurer de :

– la désactivation des services et des fonctions inutiles ou inutilisées, ou leur restriction, par exemple aux seuls utilisateurs devant accéder à ces fonctions, voire certains créneaux horaires ;
– l'authentification des utilisateurs pour l'utilisation des fonctions sensibles (par exemple : boîtes vocales, transfert vers l'extérieur, etc.) ;
– le remplacement des mots de passe par défaut (sortis de l'usine) par des mots de passe robustes et régulièrement renouvelés ;
– la désactivation de l'accès permanent de la télémaintenance en préférant plutôt la maintenance sur site supervisée ou, à défaut, l'activation temporaire et la supervision des actions de télémaintenance ;
– la synchronisation horaire du système ;
– la journalisation et la détection du trafic anormal (volume, destination) en conformité avec les obligations légales (notamment la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) ;
– l'utilisation des fonctions de filtrage ou de blocage (interdiction de certains numéros surtaxés notamment).

Une revue de la programmation téléphonique doit être organisée périodiquement.

- la mise en œuvre de codes d'accès téléphoniques : les utilisateurs doivent être sensibilisés au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale ;

- la limitation de l'utilisation du DECT :

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

### 5.6.4 Défense générique des systèmes d'information

Les mesures de défense générique suivantes doivent être intégrées dans toute procédure d'exploitation de la sécurité et mises en œuvre pour s'assurer de la vigilance de tous et garantir des actions permanentes :

- gestion dynamique de la sécurité :

– l'équipe en charge de la SSI doit procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information. Un compte-rendu hebdomadaire doit être transmis au RSSI ;

- maîtrise des matériels :

– les postes de travail sont fournis à l'utilisateur par le ministère, gérés et configurés sous la responsabilité de la sous-direction de l'informatique et des télécommunications ;
– la connexion d'équipements non maîtrisés, non administrés ou non mis à jour par la SDIT, qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles, sur des équipements et des réseaux professionnels, est strictement interdite ;

    - rappel des mesures de 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 ;
– il est recommandé de chiffrer les données contenues sur ces supports ;
– les supports contenant des données sensibles (au sens de la ligne directrice n° 4 de la PMDS) doivent être stockés dans des meubles fermant à clef ;

    - déclarer au RSSI les pertes et vols de toute ressource d'un système d'information ;
    - réaffectation des matériels informatiques :

– la procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être définie puis validée par le HFDS et mise en place par le RSSI ;
– elle doit préciser les conditions de recours à un effacement des données ;

    - déclaration des équipements nomades aptes à traiter des informations sensibles :

– l'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles dans le dossier de sécurité ;
– les usages non explicitement autorisés sont interdits ;

    - accès à distance au système d'information de l'organisme :

– les utilisateurs distants doivent s'authentifier sur le réseau de l'entité en utilisant une méthode conforme à l'annexe B3 du référentiel général de sécurité.

## *5.7 Sécurité du développement des systèmes*

Les développements logiciels doivent être menés avec une méthodologie de sécurisation du code produit ; les procédures d'exploitation de la sécurité devront à ce titre être intégrées aux cahiers des charges destinés aux développeurs. Elles seront utilisées également dans le cadre des recettes et devront préciser comment doivent être traités les points suivants :

### 5.7.1 Prise en compte de la sécurité dans le développement des logiciels

– limiter les fuites d'informations techniques sur les logiciels utilisés qui permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle ;
– réduire l'adhérence des applications à des produits ou technologies spécifiques : le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer, au-delà du respect du cadre de cohérence technique (CCT), que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en

condition de sécurité propre à l'application, il est nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée ;

- instaurer des critères de développement sécurisé : une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement ;
- intégrer la sécurité dans le cycle de vie logiciel à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette ;
- améliorer la prise en compte de la sécurité dans les développements Web (en particulier PHP) qui font l'objet de problèmes de sécurité récurrents et ont conduit à la constitution de référentiels de sécurité. Ces référentiels ont pour objectif de fixer des règles de bonne pratique à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, *etc*.). En particulier les développeurs respectent les règles du « *SANS Institute* ». Ils se réfèrent aux deux guides : « *Fundamental practices for secure software development* » Un guide référençant des pratiques de développement sécurisé) et de « l'open web application security project » (OWASP) et assurent que le code est résistant aux outils de recherche automatique de vulnérabilités ;
- calculer les empreintes de mots de passe de manière sécurisée : lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, *etc*.

### 5.7.2 Sécurisation des applications à risque

Il est recommandé pour les applications à risques de faire usage d'une solution tierce de filtrage applicatif.

# 6 LIGNE DIRECTRICE N° 4 : PROTECTION DE L'INFORMATION

## *6.1 Identification des éléments à protéger*

À tous les niveaux de responsabilité, les autorités administratives sont propriétaires des informations qu'elles génèrent et il leur revient de définir leurs besoins en sécurité en fonction de la sensibilité de ces informations.
Elles sont par ailleurs dépositaires des informations qui leur sont confiées et doivent alors leur appliquer les règles de protection nécessaires aux besoins de sécurité définis par l'autorité qualifiée en sécurité des systèmes d'informations (AQSSI), au sens de la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 approuvant la politique de sécurité des systèmes d'information de l'Etat.

### 6.1.1 Échelle des sensibilités

Afin d'aider les responsables et les maîtrises d'ouvrage à déterminer le niveau de sensibilité des informations et à définir leurs besoins de sécurité, l'échelle de besoins détaillée ci-dessous est l'échelle de référence pour l'ensemble des éléments essentiels du SAIVAJ ; une adaptation de cette échelle pour un projet particulier est possible à condition de justifier cette adaptation, et d'en référer au HFDS.

| **Confidentialité** | | | |
|---|---|---|---|
| **0**<br>**Faible ou Nul** | **1**<br>**Diffusion limitée** | **2**<br>**Diffusion restreinte** | **3**<br>**Secret** |
| L'élément essentiel peut être rendu public. | L'accès à l'élément essentiel est restreint aux personnels ou processus internes autorisés par leur fonction ou par leur appartenance à une entité organisationnelle. | L'accès à l'élément essentiel est restreint aux personnels ou processus internes autorisés par leur fonction ou par leur appartenance à une entité organisationnelle, et qui par ailleurs ont besoin d'en connaître. | Accès strictement restreint aux seuls personnels nommément désignés par la loi ou un règlement. |
| **Disponibilité** | | | |
| **0**<br>**Faible** | **1**<br>**Disponibilité sous quelques jours** | **2**<br>**Disponibilité dans la journée** | **3**<br>**Disponibilité sans délai** |
| L'élément essentiel peut être indisponible pour une longue période. | L'élément essentiel doit être disponible sous quelques jours. | L'élément essentiel doit être disponible dans la journée pour les personnes qui ont besoin d'en disposer. | L'élément essentiel doit être disponible sans délai pour les personnes qui ont besoin d'en disposer. |

| Intégrité | | | |
|---|---|---|---|
| **0**<br>**Faible** | **1**<br>**Intégrité vérifiable** | **2**<br>**Intégrité corrigible** | **3**<br>**Intégrité totale** |
| L'élément essentiel peut ne pas être intègre. | Besoin de détection du caractère intègre ou non-intègre de l'élément essentiel, sans correction nécessaire. | Besoin de détection du caractère intègre ou non intègre de l'élément essentiel, avec correction requise si besoin. | L'intégrité de l'élément essentiel doit être totale aussi bien pendant sa période d'utilisation qu'ultérieurement (ex : archivage légal ou opérationnel). |
| **Traçabilité** | | | |
| **0**<br>**Faible ou nul** | **1**<br>**Besoin pour information** | **2**<br>**Besoin de traçabilité systématique** | **3**<br>**Traçabilité légale** |
| Aucun besoin de traçabilité. | Besoin de traçabilité pour information, avec enregistrement éventuel d'une trace (non nécessairement détaillée). | Besoin de traçabilité pour information, avec enregistrement systématique d'une trace détaillée (ex : besoin commercial ou de facturation). | Besoin légal de traçabilité avec enregistrement systématique de trace comme élément de preuve indiscutable. |

### 6.1.2 Niveau de sensibilité

Les informations sensibles provenant de sources externes et qui sont munies d'un marquage de sensibilité (ex : « restreint UE », « confidentiel industrie », *etc*.) doivent être manipulées en conformité avec la réglementation en vigueur.

Chaque PSO doit définir les grands domaines de sensibilité des informations qui lui sont applicables (ex : secret de l'instruction, confidentiel personnel, confidentialité des marchés publics, *etc*.)

Les informations relevant de ces grands domaines de sensibilité seront considérées comme affectées par défaut du niveau de sensibilité du domaine donné.

Le niveau de sensibilité peut faire l'objet d'une matérialisation par un marquage visible. Pour les documents, ce marquage sera dans la mesure du possible intégré aux chartes graphiques.

Dans tous les cas, et en particulier même en l'absence de marquage, le niveau de sensibilité doit être immédiatement reconnaissable (par exemple, parce qu'il appartient à un répertoire lui-même marqué ou qu'il est traité par une application d'un domaine métier sensible).

Le niveau de sensibilité d'une information et son marquage éventuel peuvent évoluer ou être révisés en fonction du contexte d'utilisation de l'information.

### 6.1.3 Règles d'accès à des informations ou à des systèmes de communication

Il convient de définir, à tous les niveaux, des règles précisant les modalités et les habilitations nécessaires pour accéder à des informations ou à des systèmes de communication.

#### 6.1.3.1 Définition et contrôle des habilitations des personnels

L'accès aux informations sensibles doit être limité aux personnes ayant besoin d'en connaître dans le cadre de leurs fonctions et qui ont été informées des mesures de sécurité à mettre en œuvre et des responsabilités engendrées par leurs manipulations.
Les opérateurs d'importance vitale veillent au respect des règles d'attribution, de retrait et de contrôle des droits d'accès aux systèmes d'information des personnels dans chacun de leur domaine de sensibilité des informations.
En outre, ils veillent à faire respecter les règles de gestion définies par les propriétaires (organismes externes, clients, sous-traitants, *etc*.) des informations dont ils sont dépositaires.
La maîtrise d'ouvrage doit être en mesure d'attribuer des habilitations liées à l'utilisation des informations et a pour mission de définir les règles de gestion des habilitations et d'effectuer les contrôles correspondants.

#### 6.1.3.2 Accessibilité des informations (en confidentialité, intégrité, disponibilité)

L'opérateur d'importance vitale met en place les mécanismes nécessaires pour s'assurer que les informations sont exclusivement portées à la connaissance des personnes ayant besoin d'en connaître, qu'elles ne sont modifiables que par les personnes ayant le besoin de les modifier, et qu'elles ne sont rendues disponibles qu'aux personnes ayant le besoin d'en disposer.
La mise en œuvre de ces mécanismes nécessite une identification préalable des personnes ayant le besoin d'accéder à l'information.
L'opérateur d'importance vitale met en place les mécanismes adaptés pour suivre les accès, la modification ou la diffusion des informations.

#### 6.1.3.3 Répartition des rôles et responsabilités pour la définition des accès à un système d'information et du service rendu par le système d'information

- Pour l'accès à un système d'information, on doit distinguer clairement comme sur le tableau suivant :

– sur un premier axe, ce qui ressortit du décisionnel ou de la mise en œuvre ;
– sur un second axe, ce qui relève de la définition des accès au système d'information ou de la définition des accès au service rendu par le SI.

| | DECISION | APPLICATION |
|---|---|---|
| **DEFINITION DES ACCES AU SYSTEME D'INFORMATION** | ***Maîtrise d'ouvrage*** | ***Maîtrise d'œuvre*** |
| **DEFINITION DU SERVICE RENDU PAR LE SYSTEME D'INFORMATION** | ***Responsable fonctionnel*** | ***Administrateur technique*** |

- Pour les systèmes d'information dont le dossier de sécurité est de niveau 3, les emplois touchant à la maîtrise d'ouvrage (y compris l'assistance à maîtrise d'ouvrage) et à la maîtrise d'œuvre (y compris la gestion et la maintenance) du système devront être inscrits au catalogue des emplois qui peuvent nécessiter l'accès aux informations ou supports classifiés ;
- Pour chaque système d'information, la maîtrise d'ouvrage définit les profils d'utilisateur en matière de besoins de droits d'accès. La définition des profils et des droits associés doit respecter le principe du besoin d'en connaître, d'en disposer et de modifier : tout utilisateur aura exclusivement accès aux ressources et informations dont il a besoin dans l'accomplissement de sa tâche.

Chaque définition de profil doit spécifier une limite dans le temps et dans l'espace. Des profils particuliers pourront être définis pour les personnels de sociétés prestataires de service opérant sur le système d'information. La définition des profils devra prendre en compte les dispositifs planifiés de gestion des situations d'exception (absence de personnels qualifiés, vacance de poste, congés, *etc*.) et de gestion des incidents.
La maîtrise d'œuvre met en application ce que la maîtrise d'ouvrage demande. Le principe du moindre accès (profil vide par défaut) est appliqué par la maîtrise d'œuvre lors de l'ouverture et la mise en service des accès d'un personnel à un système d'information.
Le responsable fonctionnel, dans son périmètre, a la responsabilité de l'attribution nominative et de la révocation d'un profil à chaque personnel.Les profils et les droits associés sont attribués à une personne physique et sont incessibles.
Le responsable fonctionnel est chargé de la vérification et des contrôles à effectuer (identité, compétence) pour s'assurer du respect des exigences définies par la maîtrise d'ouvrage. Ces contrôles sont particulièrement nécessaires lorsqu'il s'agit de personnels de sociétés prestataires de service ;
Les personnels doivent alors donner acte formellement de leur connaissance des responsabilités relatives au profil qui leur est attribué.
La mise en œuvre de l'attribution et de la révocation d'un profil à un personnel est assurée par un administrateur technique.
Les emplois de responsable fonctionnel et d'administrateur technique sont incompatibles : ils ne peuvent être tenus par un même agent.

## *6.2 Informations relevant du secret de la défense nationale*

Le texte de référence relatif au traitement d'informations relevant du secret de la défense nationale est l'instruction générale interministérielle sur la protection du secret de la défense nationale n° 1300, portée par arrêté du Premier ministre.

### 6.2.1 Principes et organisation de la protection

#### 6.2.1.1 Rôle des autorités hiérarchiques

Le HFDS est responsable au sein du SAIVAJ de l'application des dispositions relatives à la sécurité de défense ;

- il prend les décisions d'habilitation ;
- il est responsable de la diffusion et de l'application des dispositions relatives à la sécurité de défense et à la protection du secret ;
- il veille au bon fonctionnement de la chaîne de sécurité et de défense, vérifie l'exactitude des inventaires, procède aux contrôles et inspections nécessaires et propose toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place.

Les autorités hiérarchiques assument, chacune à leur échelon et dans le cadre de leurs attributions, la responsabilité des mesures de sécurité relatives à la protection du secret. Elles établissent et transmettent au HFDS sous couvert de l'officier central de sécurité, la liste des emplois ou fonctions nécessitant l'accès à des informations ou supports classifiés.

<table>
<tr><th colspan="5">SECURITE DE DEFENSE AU SEIN DU SAIVAJ<br>REPARTITION DES RESPONSABILITES</th></tr>
<tr><th colspan="5">ADMINISTRATION CENTRALE</th></tr>
<tr><th>OIV</th><th>AUTORITE HIERARCHIQUE</th><th>PERIMETRE</th><th>OFFICIER CENTRAL DE SECURITE</th><th>OFFICIER LOCAL DE SECURITE</th></tr>
<tr><td rowspan="8">SG</td><td>Directeur de cabinet du garde des sceaux (GDS)</td><td>Cabinet du GDS</td><td colspan="2">Chef du bureau du cabinet</td></tr>
<tr><td rowspan="3">SG</td><td>SDAC</td><td colspan="2">HFDS / A</td></tr>
<tr><td>SDIT</td><td colspan="2">SDIT / A</td></tr>
<tr><td>DIJ</td><td colspan="2">RSSI</td></tr>
<tr><td>DSJ</td><td>Administration centrale<br>DSJ</td><td colspan="2">Chef de cabinet<br>CB FIP2 / A</td></tr>
<tr><td>DAP</td><td>Administration centrale<br>DAP</td><td colspan="2">Directeur de cabinet</td></tr>
<tr><td>DPJJ</td><td>Administration centrale<br>DPJJ</td><td colspan="2">Chef de cabinet</td></tr>
<tr><td>DACG</td><td>Administration centrale</td><td colspan="2">Chef de cabinet</td></tr>
<tr><td>DACS</td><td>Administration centrale</td><td colspan="2">Chef de cabinet</td></tr>
<tr><td>CE</td><td>Secrétaire général</td><td>Conseil d'État et CNDA</td><td colspan="2">Directeur de l'équipement</td></tr>
<tr><th colspan="5">SERVICES DÉCONCENTRÉS</th></tr>
<tr><td rowspan="2">DSJ</td><td>Chefs de cour ZDS</td><td>Zone de défense et de sécurité</td><td rowspan="2">Chef de cabinet<br>CB FIP2 / A</td><td>Secrétaires généraux ZDS</td></tr>
<tr><td>Chefs de cour</td><td>Cour d'appel</td><td>Secrétaires généraux</td></tr>
<tr><td>DAP</td><td>DISP</td><td>DISP</td><td>Directeur de cabinet DAP</td><td>Chef département sécurité et détention</td></tr>
<tr><td>DPJJ</td><td>DIPJJ</td><td>DIPJJ</td><td>Chef de cabinet DPJJ</td><td>Adjoint du DI</td></tr>
</table>

| CE | Secrétaire général | Autres juridictions administratives | Directeur de l'équipement | Présidents des TA et CAA |
|---|---|---|---|---|

### 6.2.1.2 Rôle des officiers centraux de sécurité

Les officiers centraux de sécurité sont les correspondants du service HFDS et des services enquêteurs. Ils ont pour mission, sous les ordres de leur autorité d'emploi, de fixer dans leur périmètre les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou supports classifiés et d'en contrôler l'application :

- ils participent à l'instruction et à la sensibilisation du personnel en matière de protection du secret ;
- ils diligentent la procédure d'habilitation ou de fin d'habilitation des personnels nommés pour assumer des fonctions inscrites au catalogue des emplois, ou quittant ces fonctions en administration centrale ;
- ils veillent à la tenue à jour du catalogue des emplois des services déconcentrés, recueillent et transmettent au HFDS, pour instruction et décision, les dossiers de demande d'habilitation issus tant de l'administration centrale que des services déconcentrés ;
- ils sont chargés de la liaison avec les services enquêteurs, du contrôle des accès aux zones protégées ;
- ils dirigent le bureau de protection du secret ; ils identifient et assurent l'enregistrement par voie informatique de l'ensemble des informations et supports classifiés émis ou reçus au niveau de leur administration centrale, et organisent l'identification et l'enregistrement des informations et support classifiés au niveau des services déconcentrés ;
- ils organisent et contrôlent la reproduction au sein des services des informations ou supports classifiés dans les conditions fixées par l'instruction générale interministérielle n° 1300 (article 48 de la version portée par l'arrêté du 30 novembre 2011) ;
- ils établissent à la demande du HFDS des états périodiques relatifs à ces missions.

### 6.2.1.3 Rôle de l'officier zonal ou régional de sécurité

L'officier zonal ou régional de sécurité est le correspondant de l'officier central de sécurité pour son ressort :

- il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret ;
- il diligente la procédure d'habilitation ou de fin d'habilitation des personnels nommés pour assumer des fonctions inscrites au catalogue des emplois ou quittant ces fonctions, veille à la tenue à jour du catalogue des emplois, recueille et transmet à l'officier central de sécurité les dossiers de demande d'habilitation de l'ensemble de son ressort ;
- il identifie et assure l'enregistrement par voie informatique de l'ensemble des informations et supports classifiés émis ou reçus.

### 6.2.1.4 Rôle de l'officier de sécurité au sein des structures déconcentrées

L'officier de sécurité est le correspondant local de la chaîne de sécurité et de défense :

- il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret ;
- il diligente la procédure d'habilitation ou de fin d'habilitation des personnels nommés pour assumer des fonctions inscrites au catalogue des emplois ou quittant ces fonctions ;
- il veille à la tenue à jour du catalogue des emplois ;
- il recueille et transmet à l'officier zonal ou régional de sécurité les dossiers de demande d'habilitation ;
- il identifie et assure l'enregistrement par voie informatique de l'ensemble des informations et supports classifiés émis ou reçus.

### 6.2.2 Règles de sécurité concernant les informations ou supports classifiés et l'habilitation des personnes ayant besoin d'en connaître

#### 6.2.2.1 Les informations ayant vocation à être classifiées

##### *6.2.2.1.1 Niveau de classification*

Le niveau de classification utilisé dans le SAIVAJ est de manière générale le niveau Confidentiel-Défense. Cependant, pour certaines politiques spécifiques (dont celles relatives à l'antiterrorisme), les niveaux supérieurs de classification peuvent être utilisés avec l'accord du HFDS.

##### *6.2.2.1.2 Informations classifiées*

- Planification de sécurité

Font en particulier l'objet d'une classification au niveau Confidentiel-Défense, sous la responsabilité de l'autorité hiérarchique, les annexes des documents de planification de sécurité comportant des éléments dont la divulgation est de nature à nuire à la défense nationale en ce qu'elle serait susceptible de favoriser une atteinte ou un préjudice à la sécurité des personnes ou de faciliter la perturbation de la continuité des missions d'importance vitale (article R. 2311-3 du code de la défense). Sont notamment visés par cette obligation les plans particuliers de protection, les plans de protection, les plans d'organisation interne, les plans de protection et d'intervention, les études de sécurité, *etc.*

- Renseignement pénitentiaire

Les informations collectées par le bureau du renseignement pénitentiaire sont classifiées par celui-ci au niveau Confidentiel-Défense.

#### 6.2.2.2 Qualification des personnes pour connaître des informations ou supports classifiés

En vertu de l'article R. 2311-7 du code de la défense, nul n'est qualifié pour connaître des informations ou supports classifiés s'il n'est habilité au niveau requis et s'il n'a besoin de les connaître. Le besoin de connaître ou d'accéder à une information classifiée est attesté par l'inscription de l'emploi considéré au catalogue des emplois.

#### 6.2.2.3 Catalogue des emplois

Tous les emplois nécessitant la connaissance d'informations classifiées doivent faire l'objet d'une inscription, par l'autorité hiérarchique, au catalogue des emplois, tant en ce qui concerne les emplois de statut public que ceux relevant d'entreprises prestataires de l'administration.

### 6.2.2.4 Forme du catalogue des emplois

| **administration centrale<br>ou<br>direction d'administration centrale<br>ou<br>cour d'appel<br>ou<br>direction interrégionale<br>ou<br>établissement pénitentiaire / direction territoriale** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N° catalogue | Grade | Fonction | Nom | Prénom | Date de naissance | Lieu de naissance | CNI (n°, date et lieu de délivrance) | N° dossier | Niveau | Date début habilitation | Date échéance habilitation | Nature et date des opérations effectuées |
| | | | | | 00/00/0000 | | 000000000000 | 0000 | CD | 00/00/0000 | 00/00/0000 | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

### 6.2.3 La procédure de classification d'informations

La décision de classifier une information a pour but de restreindre l'accès à cette information ou à ce support aux personnes préalablement habilitées et justifiant du besoin d'en connaître. Elle place donc cette information ou ce support sous la protection des dispositions des articles 413-9 et suivants du code pénal.

#### 6.2.3.1 Marquage des informations classifiées

La classification est matérialisée par l'apposition d'une mention spécifique qui permet de caractériser l'infraction pénale en cas de compromission ; le marquage d'un support papier comprend le timbre, l'identification et la pagination.
Le timbre de la mention de classification est apposé avec une encre rouge au milieu du haut et du bas de chaque page. Lorsque les documents sont établis sur poste informatique, le marquage doit être ajouté par voie électronique à l'entête et au pied de page.
L'identification se fait dès la première page avec la référence du service émetteur, la date d'émission du numéro d'enregistrement, le timbre du niveau de classification.
Chaque page est numérotée au bas de la page et mentionne le nombre total de pages.

#### 6.2.3.2 Durée de la classification

L'autorité émettrice apprécie la durée utile de classification d'une information ou d'un support. Néanmoins, l'organisation de l'inventaire annuel par l'autorité détentrice permet de procéder à une révision du besoin et du niveau de classification des informations ou supports classifiés au niveau Confidentiel-Défense. Un procès-verbal est établi à partir de l'inventaire des documents classifiés, déclassifiés ou détruits.

#### 6.2.3.3 Les obligations liées à la gestion matérielle des supports d'information classifiée

- un inventaire est effectué systématiquement à chaque mutation de personnel sous forme contradictoire, l'ancien détenteur et le nouveau apposant leur signature sur un procès-verbal ;
- la reproduction d'une information Confidentiel-Défense peut être effectuée par les autorités détentrices, à condition de conserver sur un système d'enregistrement la trace du nombre d'exemplaires reproduits et la liste des destinataires ;
- les informations ou supports classifiés sont conservés dans des coffres-forts ou des armoires fortes.

#### 6.2.3.4 Procédure à suivre pour l'expédition d'informations et de supports classifiés

- par voie postale : l'expédition des documents et supports classifiés est autorisée sur le territoire national, à la condition impérative de recourir aux opérateurs postaux proposant des moyens de transport protégés, tels que l'envoi en pli chargé avec valeur déclarée ou la lettre recommandée avec accusé de réception ;
- conditionnement : l'envoi de supports d'informations ou de supports classifiés se fait sous double enveloppe présentant des garanties de solidité de nature à assurer au maximum l'intégrité physique des supports :

- l'enveloppe extérieure, plastifiée, porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la

mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou du support qu'elle contient ;

– l'enveloppe intérieure de sécurité de bonne qualité, opaque, si possible du modèle toilé ou armé, doit interdire une ouverture ou une refermeture discrète. Elle porte le timbre du niveau de classification, la référence du support transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication du service ou de l'organisme dans lequel il est affecté.

    - sous forme électronique : la transmission par internet est rigoureusement prohibée ; la transmission électronique ne peut s'effectuer que sur le réseau spécialisé ISIS, permettant l'envoi d'informations classifiées jusqu'au niveau Confidentiel-Défense.

### 6.2.4 La procédure d'habilitation

#### 6.2.4.1 Sens montant : du candidat à l'autorité d'habilitation

##### *6.2.4.1.1 Rôle du candidat à l'habilitation*

- à la prise de poste :

– renseigne le formulaire 94A (de la page 2 à la page 7) directement sur un poste informatique ; la page 1 du formulaire est réservée aux services administratifs. La notice individuelle a un caractère déclaratif, les renseignements portés sont de la seule responsabilité du candidat ; il doit être répondu à l'ensemble des questions ;
– insère numériquement sa photo d'identité (ne pas la coller ou l'agrafer) ;
– enregistre sa demande et peut ainsi en conserver une copie dématérialisée ;
– adresse le formulaire ainsi renseigné sur ordinateur et non signé à l'officier local de sécurité, ainsi qu'une copie signée de sa demande sous format papier ;
– renseigne, date, signe et adresse le formulaire papier d'engagement de responsabilité (1er volet : prise de poste) à l'officier local de sécurité.

- Au départ du poste :

– renseigne, date, signe et adresse le formulaire papier d'engagement de responsabilité (2e volet : départ du poste) à l'officier local de sécurité.

##### *6.2.4.1.2 Rôle de l'officier local de sécurité*

– renseigne sur écran, à la page 1 du formulaire numérique 94A la rubrique « zone réservée à l'organisme demandeur » : organisme demandeur, numéro concerné du catalogue des emplois, coordonnées de l'officier local de sécurité, nature de la décision demandée, niveau d'habilitation demandé, fonctions exercées, demande éventuelle de mise en œuvre de la procédure d'urgence ;
– renseigne le tableau du catalogue des emplois ;
– adresse le dossier numérisé à l'officier régional de sécurité ;
– adresse le formulaire papier d'engagement de responsabilité à l'officier régional de sécurité.

##### *6.2.4.1.3 Rôle de l'officier zonal ou régional de sécurité*

– renseigne le tableau du catalogue régional des emplois ;
– adresse le dossier numérisé à l'officier central de sécurité ;
– adresse le formulaire papier d'engagement de responsabilité à l'officier régional de sécurité.

##### *6.2.4.1.4 Rôle de l'officier central de sécurité*

– renseigne sur la première page du formulaire numérique 94A l'avant dernière rubrique « à remplir par l'officier de sécurité… » ;
– renseigne le tableau du catalogue central des emplois ;
– adresse le dossier numérisé à la cellule d'appui du HFDS.

#### *6.2.4.1.5 Rôle de la cellule d'appui du HFDS*

– procède à l'instruction du dossier de demande ;
– soumet la décision d'habilitation à la signature du HFDS ;
– renseigne le tableau du catalogue ministériel des emplois.

### 6.2.4.2 Sens descendant : de l'autorité d'habilitation à la personne habilitée

#### *6.2.4.2.1 Rôle de la cellule d'appui du HFDS*

– adresse les données relatives à l'habilitation (numéro de la décision, niveau, date d'effet, date d'échéance) à l'officier central de sécurité ;

#### *6.2.4.2.2 Rôle de l'officier central de sécurité*

– adresse les données relatives à l'habilitation (numéro de la décision, niveau, date d'effet, date d'échéance) à l'officier central de sécurité ;
– renseigne le tableau du catalogue central des emplois ;

#### *6.2.4.2.3 Rôle de l'officier régional de sécurité*

– adresse les données relatives à l'habilitation (numéro de la décision, niveau, date d'effet, date d'échéance) à l'officier local de sécurité ;
– renseigne le tableau du catalogue régional des emplois ;

#### *6.2.4.2.4 Rôle de l'officier local de sécurité*

– renseigne le tableau du catalogue régional des emplois ;
– notifie oralement la décision d'habilitation à la personne concernée.

## 6.2.5 Durée de validité de l'habilitation

La durée de validité de l'habilitation est liée à la durée d'occupation du poste qui a justifié sa délivrance. Elle cesse lorsque l'intéressé quitte son emploi.
La durée de validité de l'habilitation est au plus de 7 ans au niveau Secret-Défense et de dix ans au niveau Confidentiel-Défense.

## 6.2.6 Conditions posées par la commission nationale de l'informatique et des libertés

Les traitements, sous forme de répertoires automatisés sont mis en œuvre par la cellule d'appui du HFDS. Conformément notamment à la délibération de la commission nationale de l'informatique et des libertés n° 2011-298 du 21 septembre 2011, ils répondent aux caractéristiques suivantes :

– données inclues : identité des personnes physiques candidates à l'habilitation ou habilitées (nom, prénom, sexe, date et lieu de naissance, nationalité et références des documents d'identité présentés), vie professionnelle (organisme d'affectation, fonctions occupées, titre ou grade, coordonnées professionnelles), éléments techniques de gestion du dossier (identification, instruction, durée de validité et suivi de la décision d'habilitation) ;

- données exclues : éléments des enquêtes administratives réalisées dans le cadre de la procédure d'habilitation, à l'exception du sens de l'avis de sécurité qui en est issu ;
- durée de conservation : un an après la fin de l'avis de sécurité émis par le service enquêteur ;
- destinataires des données : agents habilités de la cellule d'appui du HFDS et des autorités ayant reçu délégation à cet effet, en fonction de leurs attributions respectives et du besoin d'en connaître. Ils ne peuvent communiquer le résultat de la procédure d'habilitation, dans la limite du besoin d'en connaître, qu'aux seuls services de ressources humaines et informatiques, ainsi qu'à la chaîne hiérarchique du candidat à l'habilitation ;
- information des personnes par mention dans le formulaire de demande d'habilitation rempli par l'intéressé ; le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 ne s'applique pas. Les droits d'accès et de rectification s'exercent directement auprès de la cellule d'appui du HFDS ;
- sécurité : des mesures de traçabilité des accès et des consultations du traitement sont mises en œuvre.

### 6.2.7 La protection du secret dans les contrats

On pourra se reporter au titre VI de l'instruction générale interministérielle n° 1300 dans la version portée par l'arrêté du 30 novembre 2011.

#### 6.2.7.1 Obligations de l'autorité contractante

Tout contrat qui implique l'accès aux informations ou supports classifiés comporte des clauses de protection du secret précisant les obligations des contractants (voir par exemple les clauses types figurant en annexe 10 de l'instruction générale interministérielle n° 1300 dans la version précitée).

Ces obligations sont relatives à la protection des informations que le titulaire, au titre du contrat, serait d'une part amené à connaître ou d'autre part à détenir.

Dès le début de la procédure de passation du contrat, l'autorité contractante informe les futurs candidats du délai imparti pour fournir les documents nécessaires à l'habilitation et, si le contrat nécessite la détention d'informations classifiées, pour faire procéder à l'évaluation de l'aptitude physique de l'entreprise à cette détention. Ce délai ne peut être inférieur à 15 jours à compter de la date de l'information communiquée par l'autorité contractante.
Lorsque le dossier est incomplet, l'autorité contractante informe les soumissionnaires des pièces manquantes qui devront être fournies avant l'expiration du délai fixé.

#### 6.2.7.2 Communication d'informations classifiées en phase précontractuelle

Dès lors que la prise de connaissance d'informations classifiées est nécessaire pour l'élaboration et la soumission de l'offre, les procédures d'habilitation de l'entreprise et de ses personnels peuvent être initiées.

#### 6.2.7.3 Procédure à suivre

- l'autorité contractante organise l'information des candidats et la réception des pièces ;
- les demandes d'habilitation de personnes ou d'entreprises sont transmises au HFDS sous couvert de l'officier de sécurité ;
- le HFDS informe l'officier de sécurité de la décision prise sur l'habilitation.

## *6.3 Échanges d'informations*

### 6.3.1 Echanges d'informations classifiées au titre du secret de la défense nationale

Les informations classifiées peuvent être transmises par voie postale dans les conditions rappelées en 6.2.3.4. Elles ne peuvent être transmises par voie électronique qu'à l'aide de moyens dédiés :

#### 6.3.1.1 Réseau RIMBAUD (réseau interministériel de base uniformément durci)

Le secrétariat général de la défense et de la sécurité nationale est chargé de fournir aux autorités gouvernementales des moyens de communication sécurisés dont le fonctionnement doit être assuré en toutes circonstances.

Le réseau téléphonique RIMBAUD est un réseau résilient à très haute disponibilité qui réunit les services d'importance vitale. Il se caractérise par l'utilisation d'infrastructures dédiées, déconnectées des opérateurs publics. Progressivement équipé de terminaux chiffrant TEOREM, il permet de protéger les communications jusqu'au niveau Secret-Défense.

Dans un contexte marqué par la fragilité des réseaux ouverts au grand public et des terminaux de communication du commerce, ainsi que par la multiplication des actes de malveillance (écoutes ou saturation), le réseau sécurisé RIMBAUD doit être utilisé dans le cadre des communications de travail courant entre services d'importance vitale pour les échanges d'informations sensibles : soit portant une mention particulière de confidentialité : « Confidentiel-Personnel », ou « Diffusion-Restreinte », soit classifiées au niveau Confidentiel-Défense ou Secret-Défense.

##### *6.3.1.1.1 Les lignes RIMBAUD*

Le ministère de la justice est doté de trois périmètres RIMBAUD :
- réseau de l'administration centrale ;
- réseau des services judiciaires ;
- réseau des services pénitentiaires.

Les demandes de création de lignes RIMBAUD, ou de modification de l'abonnement RIMBAUD, sont matérialisées par l'envoi du formulaire numérisé spécifique fourni par le SGDSN et l'ANSSI et mis à disposition sur le site intranet du HFDS ; la DIT ou le service concerné l'adresse complété à la cellule d'appui du HFDS : hfds@justice.gouv.fr

L'ouverture d'une ligne Rimbaud déclenche la commande d'un terminal TEOREM.

##### *6.3.1.1.2 Les postes TEOREM (téléphone cryptographique pour réseau étatique et militaire)*

- composants du téléphone TEOREM :

Les postes téléphoniques TEOREM comportent des dispositifs cryptographiques permettant le chiffrement des informations et constituent des articles contrôlés de la sécurité des systèmes d'information (ACSSI) qui nécessitent la mise en place de règles de gestion et de sécurité. Une traçabilité des composants du système est centralisée au niveau de l'Etat par l'ANSSI et doit être observée à tous les échelons administratifs concernés par le déploiement du TEOREM.

Les postes TEOREM comportent une base d'accès réseau (BAR) et un combiné reliés par un câble torsadé :

- le numéro de la BAR est indiqué sur la quatrième ligne de l'étiquette collée sous le socle de l'appareil (les six derniers chiffres) ;
- le numéro de série du combiné est inscrit au dos de l'appareil, sous la batterie extractible ;
- le numéro de la micro carte SD se trouve sur la carte insérée dans la fente aménagée sur le côté droit du combiné.

#### *6.3.1.1.3 Habilitation de la chaîne RIMBAUD au secret de la défense nationale*

Tous les personnels composant la chaîne RIMBAUD (ensemble des personnels SDIT concernés, ensemble des utilisateurs) doivent adresser à l'officier de sécurité de leur service un dossier de demande d'habilitation au secret de la défense nationale :

- administration centrale : cellule d'appui du HFDS (hfds@justice.gouv.fr) ;
- services judiciaires : chefs de cour de zone de défense et de sécurité, puis officier de sécurité de la DSJ (habilitations.dsj@justice.gouv.fr) ;
- services pénitentiaires : cabinet de la directrice de l'administration pénitentiaire, (david.langlois@justice.gouv.fr).

#### *6.3.1.1.4 Acheminement du TEOREM*

La gestion de la chaîne TEOREM est centralisée au ministère de la justice par la cellule d'appui du HFDS (hfds@justice.gouv.fr) qui tient le rôle de point de contact avec le SGDSN pour l'approvisionnement et le maintien en condition opérationnelle des matériels, et assure la comptabilité centrale des ACSSI déployés au sein du ministère.

Le déploiement des postes TEOREM et leur retour vers la cellule d'appui du HFDS sont assurés par la SDIT (coordonnateur des DIT : guy.cohen@justice.gouv.fr) avec le concours des départements informatique et télécommunications des plateformes interrégionales de la justice.

Lors de leur transport :

- il importe que les postes TEOREM d'une part, et leur code secret de transport (enveloppe scellée) d'autre part, cheminent séparément ;
- tout transport d'un poste TEOREM doit être accompagné d'un bordereau type (disponible sur le site du HFDS) reprenant les éléments de comptabilité des ACSSI et signé de l'autorité responsable du matériel.

#### *6.3.1.1.5 Mise en service du TEOREM*

Lors de sa remise du matériel à l'autorité, le personnel SDIT habilité :

- procède à l'installation matérielle en veillant à positionner le poste à une distance de 50 cm au moins des autres moyens de communication ;
- introduit le code porteur secret contenu dans l'enveloppe scellée à l'aide du clavier numérique du combiné ;
- détruit à la fin de l'opération la feuille comportant le code porteur secret et établit un procès verbal de destruction (procès-verbal type disponible sur le site du HFDS) signé adressé à la cellule d'appui du HFDS ;

L'autorité dépositaire du matériel :

- introduit son code PIN personnel composé de quatre chiffres à l'aide du clavier numérique du combiné ;

– ce code PIN constitue une donnée classifiée, personnelle, qui doit être protégée (à mémoriser ou à inscrire sur un support archivé classifié).

#### *6.3.1.1.6 Fonctionnement du poste TEOREM*

Le poste TEOREM doit être allumé, et l'autorité dépositaire du matériel doit régulièrement s'authentifier en introduisant son code PIN personnel.

#### *6.3.1.1.7 Panne du poste TEOREM*

Lorsqu'une ligne ne fonctionne pas, il convient de la tester avec un poste clair pour déterminer si le problème vient de la ligne ou du terminal ; il est également possible de contacter le service support RIMBAUD assuré par l'opérateur France Télécom, aux numéros suivants :

– depuis un poste classique (numéro gratuit) : 08 00 25 03 13 ;
– depuis un poste sur une ligne RIMBAUD : 203 113.

Si la panne du terminal TEOREM est avérée, ou si le code PIN a été perdu par l'autorité détentrice, le personnel SDIT habilité :

– Informe la cellule d'appui HFDS et l'officier central de sécurité du retrait du matériel et de la nécessité de procéder à la commande du matériel de remplacement ;
– reconditionne le TEOREM dans son emballage et le retourne à la SDIT (coordonnateur des DIT) accompagné d'un bordereau signé reprenant le nom et la fonction de l'autorité d'affectation du matériel, le numéro de la ligne RIMBAUD ainsi que la comptabilité des ACSSI ;

Pendant la durée de l'indisponibilité du matériel, le poste TEOREM peut être remplacé par un ancien combiné RIMBAUD, qui ne pourra cependant permettre que des communications non cryptées.

Les officiers centraux de sécurité de la DSJ et de la DAP doivent être tenus informés de toutes difficultés liées à ces matériels.

### 6.3.1.2 Transmission de données

Le ministère de la justice dispose de l'intranet ISIS qui permet d'échanger des informations classifiées jusqu'au niveau Confidentiel-Défense et présente des garanties élevées de résilience qui lui confèrent les caractéristiques d'un outil de gestion de crise.

Ce moyen de transmission de données peut être d'usage collectif, chaque usager disposant d'une carte personnelle d'accès et d'un code PIN, le poste de travail pouvant être partagé de manière sécurisée.

Trois filières ayant vocation à être desservies ont été identifiées :

– administrations centrales ;
– cours d'appel de zone de défense et de sécurité ;
– directions interrégionales des services pénitentiaires.

## 6.3.2 Échanges d'informations sensibles

Les consignes gouvernementales rappellent que dans leur majorité, les informations manipulées ou échangées au sein de l'administration notamment par les autorités, sont sensibles, et que leur divulgation peut s'avérer préjudiciable aux intérêts de la Nation.

Les règles suivantes doivent en conséquence être rigoureusement observées :

– l'usage d'équipements informatiques personnels (BYOD) est interdit ;
– l'utilisation de *smartphones* du commerce, sans dispositif de sécurité agréé par l'ANSSI, est interdit, tant pour le transport de la voix que des données ;

– l’usage de messageries personnelles, et plus particulièrement celles fournies par des tiers ne pouvant garantir l’application exclusive de la loi française, est interdit ;
– le renvoi automatique d’une messagerie professionnelle vers une messagerie personnelle est interdit.

En outre :
– l’échange d’informations sensibles par SMS est interdit ;
– s’agissant des communications téléphoniques, l’utilisation d’un téléphone fixe plutôt que d’un téléphone mobile est recommandée.

Les échanges d'informations sensibles avec les partenaires (administrations, auxiliaires de justice, prestataires) doivent bénéficier d'un cadre adapté aux risques identifiés.

Des procédures doivent être définies au sein de chaque OIV et les outils doivent être mis à disposition pour permettre de répondre aux besoins de confidentialité, d'intégrité, de disponibilité et de traçabilité, en particulier pour :
– la messagerie électronique ;
– les échanges de fichiers volumineux ;
– l'interconnexion directe de systèmes d'information.

### 6.3.3 Cadre contractuel pour les échanges sécurisés de données avec des tiers

Tous les échanges sécurisés de données devront être conformes au référentiel général d'interopérabilité (RGI) et au référentiel général de sécurité (RGS).

Ces échanges de données devront se faire dans un cadre contractuel formalisé qui traitera notamment des points suivants :
– la responsabilité de la gestion des flux d'échanges ;
– les procédures de sécurité utilisées pour les échanges ;
– les standards de structuration des données ;
– les responsabilités en cas de perte des informations ;
– les mesures spécifiques pour la protection des clés cryptologiques (chiffrement, authentification, signature).

En cas d'appel d'offre pour des opérations confiées à des tiers, le cahier des charges comprendra des spécicifications :

- relatives à l’échange de données ;
- liées aux risques sur des informations dont le ministère de la justice est propriétaire ou dépositaire ;
- liées aux risques sur des informations dont le prestataire est propriétaire ou dépositaire.

### 6.3.4 Cadre contractuel avec les prestataires de services externes

Tous les contrats ou conventions passés avec des prestataires de services externes doivent permettre au SAIVAJ de garder la maîtrise pleine et entière de son système d’information. Ils doivent notamment mentionner le devoir de coopération des prestataires pour :

– les contrôles et audits externalisés, en particulier pour des tests de vulnérabilité ;

– la gestion des incidents : réactivité et transparence sont demandés au prestataire pour répondre aux requêtes de la maîtrise d'ouvrage, en particulier pour la remise des éléments de traçabilité des opérations ou des accès au système d'information ;
– l'exécution des plans de continuité d'activité, y compris les exercices prévus par ces plans.

En cas d'appel d'offre pour l'externalisation de services à des tiers, le devoir de coopération du prestataire devra être clairement stipulé dans le cahier des charges.

Des procédures particulières doivent être définies pour assurer la mise en œuvre des procédures de sécurité relatives aux moyens de transmission protégés.

### 6.3.5 Risques de signaux compromettants

Les opérateurs doivent limiter les risques d'interception de communication pouvant résulter de l'écoute éventuelle de signaux compromettants parasites (rayonnement électromagnétique) ou non parasites (technologies sans fil) ou encore résultant de l'activation inopportune de fonctionnalités propres aux matériels mis en œuvre.

Il est rappelé que la protection contre les signaux compromettants est obligatoire pour le traitement d'informations classifiées (IGI n° 1300).

Pour les systèmes d'information dont le dossier de sécurité est de niveau 2 ou 3, la menace via l'exploitation des signaux parasites compromettants est prise en compte dans l'analyse de risque.

# 7 LIGNE DIRECTRICE N° 5 : ASSURER LA PERMANENCE DE LA CAPACITÉ DE GESTION DE CRISE

## *7.1 Organisation interministérielle*

- Textes de référence :

– circulaire du Premier ministre n° 5567/SG du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures ;
– note n° 548/SGDSN/PSE/PSN du 13 novembre 2013 - Eléments de doctrine pour la fonction communication.

### 7.1.1 Rappel des responsabilités gouvernementales pour la préparation et la gestion des crises majeures

Afin d'assurer la protection de la population et du territoire, de maintenir le fonctionnement des pouvoirs publics et d'assurer la continuité de la vie de la Nation :

#### 7.1.1.1 La direction politique et stratégique des crises majeures est assurée par le Premier ministre en liaison avec le Président de la République

Le Président de la République « *assure par son arbitrage, le fonctionnement régulier des pouvoirs publics ainsi que la continuité de l'État* » (article 5 de la Constitution). Il dispose du conseil de défense et de sécurité nationale qui arrête les décisions en matière de direction politique et stratégique de réponse aux crises majeures (article L. 1111-3 du code de la défense).
Le Premier ministre « *dirige l'action du Gouvernement* » (article 20 de la Constitution). A ce titre, il « *prépare et coordonne l'action des pouvoirs publics en cas de crise majeure* » (article L. 1131-1 du code de la défense).

#### 7.1.1.2 Les ministres qui ont une responsabilité particulière dans la préparation et la conduite des crises

Le ministre de la défense est responsable de l'anticipation et du suivi des crises intéressant la défense. Il est responsable de la préparation et de la mise en œuvre de la politique de défense (article L.1142-1 du code de la défense). Le chef d'état-major des armées est responsable de l'emploi des forces, sous l'autorité du Président de la République et du Gouvernement (article R. 3121-1 du code de la défense).
Le ministre de l'intérieur est responsable de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile. Il est chargé de la conduite opérationnelle des crises sur le territoire de la République (article L. 1142-2 du code de la défense). Il doit également, au titre de la préparation à la gestion des crises, s'assurer de la transposition et de l'application au niveau déconcentré des plans gouvernementaux.
Le ministre des affaires étrangères et européennes coordonne la gestion des crises extérieures ainsi que la planification civile de celles-ci avec le concours de l'ensemble des ministères et des services de l'État concernés (article L. 1142-6 du code de la défense). Il traduit, dans l'action diplomatique au niveau européen et au niveau international, les priorités de la stratégie de sécurité nationale et de la politique de défense.

#### 7.1.1.3 La contribution des autres ministres à la préparation et à la conduite des crises

« *Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge* » (article L. 1142-1 du code de la défense). Cette responsabilité est globale et nécessite que les ministres s'organisent, dans leur champ de compétence ministérielle, pour apporter leur contribution à l'action du Gouvernement, aussi bien dans la conduite de la crise que dans la mise en œuvre des politiques de prévention. A cette fin, ils mobilisent autant que nécessaire les opérateurs de leurs secteurs d'activité pour l'analyse et la résolution des crises.
Le ministre chargé de l'économie prépare l'exécution de la politique de sécurité économique. Il prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation (article L. 1142-3 du code de la défense).
Le ministre chargé de la santé est responsable de l'organisation et de la préparation du système de santé et des moyens sanitaires nécessaires à la connaissance des menaces sanitaires graves, à leur prévention, à la protection des populations contre ces dernières, ainsi qu'à la prise en charge des victimes. Il contribue à la planification interministérielle en matière de défense et de sécurité nationale en ce qui concerne son volet sanitaire (article L. 1142-8 du code la défense).
Les ministres chargés de l'environnement, des transports, de l'énergie et de l'industrie sont responsables, chacun en ce qui le concerne, de la satisfaction des besoins de la défense et de la sécurité nationale et, en toutes circonstances, de la continuité des services (article L. 1142-9 du code de la défense).

#### 7.1.1.4 Convocation de la CIC

Pour exercer sa responsabilité dans la direction de crise, le Premier ministre s'appuie sur un dispositif gouvernemental structuré, assuré par une cellule interministérielle de crise ; le Premier ministre peut confier la conduite opérationnelle de la crise à un ministre qu'il désigne en fonction de la nature des événements, du type de crise ou de l'orientation politique qu'il entend donner à son action, la conserver à son niveau, ou prendre à son compte tout ou partie de la conduite opérationnelle, en liaison avec le Président de la République . La conduite opérationnelle est en principe confiée au ministre de l'intérieur lorsque la crise a lieu sur le territoire national ou au ministre des affaires étrangères et européennes pour les crises extérieures.
La décision de constituer une CIC peut être prise dès la survenance d'une crise ou durant son développement.

#### 7.1.1.5 Rôles dévolus aux différentes autorités gouvernementales au sein de la CIC

- Le Premier ministre, en liaison avec le Président de la République, fixe :

– l'objectif à atteindre en sortie de crise ;
– les impératifs politiques, les priorités et les contraintes majeures ;
– la stratégie de relations internationales ;
– la stratégie de communication gouvernementale.

- Le ministre chargé de la conduite opérationnelle, en s'appuyant sur l'ensemble des ministères représentés en CIC, assure pour le compte du Premier ministre :

– la centralisation de toutes les informations en relation avec la crise ;
– l'analyse de ces informations ;
– la conception des scénarios d'anticipation ;
– la préparation des décisions ;
– la coordination interministérielle dans la mise en œuvre des décisions gouvernementales.

A ce titre, il organise les travaux de la CIC pour apporter au Premier ministre des points de situation, des évaluations, il propose des décisions et fournit des éléments d'anticipation et des propositions de choix stratégiques :

- la direction de crise, dans sa dimension politique et stratégique, est assurée par le Premier ministre qui s'appuie sur le secrétariat général de la défense et de la sécurité nationale, sur le service d'information du Gouvernement, sur le secrétariat général des affaires européennes et sur le secrétariat général de la mer ;
- le SGDSN assure le secrétariat des réunions de crise, formalise les décisions qui y sont prises et les notifie à la CIC ; dès la réunion de la CIC, le SGDSN met en place une fonction de retour d'expérience, permettant d'améliorer la qualité de la réponse gouvernementale.

#### 7.1.1.6 Organisation de la CIC

Le dispositif de la CIC, structuré par les trois fonctions essentielles à l'organisation de la gestion de crise (situation, décision et communication) permet de recueillir l'ensemble des informations utiles dans un cadre interministériel et d'y développer la capacité d'analyse nécessaire à la prise de décision.

##### *7.1.1.6.1 La fonction « situation »*

La fonction « situation » assure la mise en commun de l'ensemble des informations nécessaires à l'appréciation de la situation et de son évolution. Elle comporte deux sous-ensembles auxquels les ministères affectés par la crise participent :

- les opérations : synthèse de l'information sur la situation, transmission des décisions à destination des centres opérationnels nationaux, zonaux, voire départementaux, tenue de la main courante ;
- l'anticipation : travaux sur des horizons temporels de plus en plus éloignés afin d'alimenter une réflexion prospective permettant d'anticiper la sortie de crise et de formuler des propositions d'action à la fonction « décision ».

##### *7.1.1.6.2 La fonction « décision »*

La fonction « décision » prend des décisions pour la conduite de la crise, pour ce qui relève de son niveau d'appréciation, et soumet au Premier ministre les propositions d'actions qui relèvent de choix de conduite de niveau stratégique ainsi que les éventuels arbitrages :

- elle donne les directives nécessaires à la mise en œuvre des décisions prises en CIC ou validées par le Premier ministre et s'assure de leur exécution ;
- elle établit systématiquement les relevés des décisions prises et les transmet pour mise en œuvre.

##### *7.1.1.6.3 La fonction « communication »*

La mobilisation systématique des communicants en formation interministérielle et adaptée au format d'activation de la CIC (en fonction de la typologie de la situation à laquelle l'État doit faire face) vise à garantir la recherche permanente de cohérence de la parole de l'État.

Positionnement

Le ministre chargé de la conduite opérationnelle, en s'appuyant sur l'ensemble des ministères représentés en CIC, sur le SIG, sur la fonction « communication » de la CIC et sur l'ensemble des services communication des ministères mis en réseau, assure pour le compte du Premier ministre :

- la centralisation et l'analyse de toutes les informations relatives à la perception de la crise et aux attentes du public et des médias sur l'action des pouvoirs publics au niveau national et international ;

– la préparation d'une stratégie et d'un plan de communication gouvernementaux et la coordination interministérielle dans leur mise en œuvre.

La fonction « communication » apporte sa contribution à la stratégie générale de réponse à la crise. A ce titre, elle participe au débat au sein de la fonction « décision » qu'elle éclaire sur les attentes de l'opinion en termes d'actions à conduire.

Elle enrichit également le travail d'analyse et d'élaboration des propositions de la fonction « situation », sur la base de points de situation réguliers réalisés conjointement.
Ces points visent à actualiser ;
– le contenu des messages proposés par les communicants ;
– le travail de synthèse réalisé par la fonction « situation » ;
– la bonne connaissance de la situation par la fonction « communication ».

Lignes d'action

La fonction « communication » permet, d'une part, d'apprécier la perception de la crise par l'opinion publique et de mesurer les attentes des citoyens, des opérateurs et des médias vis-à-vis des pouvoirs publics et, d'autre part, d'informer sur l'événement et les mesures prises, de diffuser les recommandations nécessaires.
Elle joue un rôle de coordination et d'impulsion des agents en charge de la communication dans les ministères concernés.

- Identification de la perception et des attentes des différents acteurs :

– éclairages sur la pression que peut exercer par les médias, l'expression publique sous ses différentes formes et la perception par la population de l'action des pouvoirs publics pouvant avoir un impact sur la gestion de la crise ;
– éclairages sur la couverture médiatique à l'étranger et l'expression de l'opinion internationale.

- Proposition d'une stratégie de communication gouvernementale et mise en œuvre *via* un plan de communication :

La fonction « communication » accompagne la mise en œuvre des décisions prises en proposant une politique de communication adaptée (stratégie de communication) et en la déclinant par la réalisation de directives de communication (plan de communication) accompagnées d'éléments de langage.
La stratégie de communication précise :
– le contexte (situation réelle, état de l'opinion publique) ;
– les enjeux de communication corrélés aux objectifs opérationnels ;
– les axes de communication ;
– les écueils à éviter

La fonction « communication » est pleinement intégrée aux travaux d'anticipation et de suivi de la situation conduits par la CIC, afin de participer à l'élaboration de la stratégie générale de gestion de la crise. Elle propose à la fonction « décision » les priorités en matière de communication qui contribuent à l'atteinte des objectifs de résolution de la crise ; ces priorités peuvent être amenées à évoluer en fonction du développement de la crise.
La fonction « communication » décline la stratégie de communication gouvernementale à travers un plan de communication validé par la fonction « décision » ; ce plan est un instrument de cohésion de la communication gouvernementale dans la durée. Adapté au fur et à mesure de l'évolution de la crise, il décrit les actions concrètes de communication conduites par la CIC, les différents ministères et les principaux opérateurs.

Le plan de communication précise :
- les objectifs de communication ;
- l'identification des cibles ;
- les messages et leurs tempos ;
- le choix des canaux de transmission des messages (Internet, presse écrite, télévision, radio, *etc*.) ;
- les supports de communication les plus adaptés à la situation (communiqués de presse, fiches, articles pour Internet, dépliants, affiches, *etc*.)
- la coordination des productions de communication entre la CIC, les différents ministères, et les principaux opérateurs ;
- la priorisation des actions de communication ;
- la coordination des prises de parole dans les médias ;
- l'échéancier des actions de communication et les effets majeurs associés (jalons de communication) ;
- les éléments de langage figurent en annexe du plan de communication.

La fonction « communication » s'assure de la bonne application du plan de communication. A cette fin, elle coordonne les actions de communication réalisées par les différents acteurs de la crise, réalise une analyse de situation et fait effectuer les ajustements nécessaires pour adapter la posture de communication.

Organisation

- La direction de la fonction « communication » :

Le pilote de la fonction communication est le ministre en charge de la conduite opérationnelle de la crise, qui peut déléguer cette fonction au porte-parole de son ministère (le porte-parole du ministère en charge des affaires étrangères est toujours compétent pour traiter sa matière) ; il remplit également la fonction de directeur de publication des diverses communications déposées par la CIC. Pour la mise en œuvre de la fonction « communication », il s'appuie sur les services communication de l'État.

- Le service d'information du Gouvernement :

Le SIG, par l'intermédiaire de son directeur ou du département communication de crise et territoriale de l'État, conseille la direction de crise (la direction de crise, dans sa dimension politique et stratégique, est assurée par le Premier ministre, qui s'appuie sur le SGDSN, le SIG, le SGAE et le SG mer).
Il participe également à la CIC où s'agissant du volet communication, il assure la liaison avec le cabinet du Premier ministre, voire les cabinets ministériels, si le premier ministre décide de conserver à son niveau la conduite opérationnelle de la crise.
Par ailleurs, le SIG met à disposition de la fonction « communication » un certain nombre de moyens :
- des notes d'alerte régulières sur la pression médiatique, l'expression publique sur Internet et les réseaux sociaux, et sur l'état de l'opinion (études et sondages traitant de la crise en précisant les sources, la tonalité, le niveau d'inquiétude, la typologie des questions journalistiques, la perception de l'action de l'État, les signaux forts et faibles sur l'émergence des tendances) ;
- un site interministériel d'information de la population en situation de crise (www.info-crise.gouv.fr) administré par le SIG (mise en ligne, ergonomie, gestion du fonctionnement) et dont le porte-parole du ministère en charge de la conduite opérationnelle de la crise est le directeur de publication ;
- le centre de contact interministériel de crise multi-canal INFOCRISE dont l'activation et les modalités de mise en œuvre sont décidées en réunion interministérielle.

- La direction ou délégation à la communication du ministère chargé de la conduite de la crise :

Elle assure le fonctionnement de la cellule « communication ». La fonction « communication » est systématiquement renforcée par les services de communication des autres ministères concernés ; le périmètre de la participation des ministères est défini en fonction de la nature de la crise.

- Les services de communication des ministères concernés par la crise :

Si la CIC peut être amenée à réaliser ses propres actions de communication, en aucun cas elle ne se substitue aux actions de communication relevant de la responsabilité des différents ministères et des autorités territoriales qui à leur niveau continuent d'assurer la liaison avec les différentes cibles (média, partenaires, associations, *etc*.).

Les représentants des services de communication des ministères concernés par la crise présents en CIC :
- participent pleinement à l'élaboration de la stratégie et du plan de communication ;
- assurent la coordination en matière de communication avec leur ministère (HFDS et centre opérationnel) ;
- s'assurent de la mise en œuvre du plan de communication par leur ministère ainsi que par les opérateurs et institutions qui sont sous sa tutelle ;
- mettent à disposition de la fonction « communication » des informations et éléments de langage propres à l'activité et aux responsabilités de leur ministère.

Les différents supports de communication sont réalisés au sein des ministères concernés, en application de la stratégie et du plan de communication. Une synthèse est réalisée si nécessaire par la fonction « communication ».

- Les services de communication des opérateurs concernés :

La sollicitation des opérateurs dans la gestion de la crise est de la responsabilité de leur ministère de tutelle. Cependant, en fonction de la nature de la crise, des circonstances et des plans mis en œuvre, les services de communication des opérateurs peuvent être amenés à participer, ponctuellement ou dans la durée, à l'armement de la fonction « communication », en mettant à sa disposition les connaissances et supports de communication nécessaires.

- Les experts et spécialistes :

Pour assurer la crédibilité de la parole de l'État et pour mettre à la disposition de la population plusieurs sources d'information reconnues et officielles, les ministères (voire la CIC) peuvent dans leur domaine de responsabilité s'appuyer sur un réseau d'experts ou de spécialistes reconnus. Leur contribution peut être mise à profit de la fonction « communication » qui sollicitera les ministères à cet effet.

## *7.2 Organisation du SAIVAJ*

### 7.2.1 Textes de référence

- Article L. 1141-1 du code de la défense :
  « *Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge.* »

– Article L 1142-7 du code de la défense :
« *Le ministre de la justice assure en toute circonstance la continuité de l'activité pénale ainsi que l'exécution des peines.*
*Il concourt, par la mise en œuvre de l'action publique et l'entraide judiciaire internationale, à la lutte contre les atteintes aux intérêts fondamentaux de la Nation.* »

### 7.2.2 Événements de sécurité et situations de crise

Les événements de sécurité visés par la PMDS résultent d'incidents ou d'accidents qui surviennent dans le fonctionnement des services, plus ou moins importants par eux-mêmes, affectant les personnes ou les biens, résultant d'une ou de plusieurs causes, et qui peuvent avoir des conséquences négatives en matière de continuité des services ou plus simplement altérer temporairement l'ordre de fonctionnement habituel des services.

Ils peuvent trouver leur source au sein des services de l'administration centrale du ministère de la justice ou de ses services déconcentrés, du réseau du Conseil d'État et des autres juridictions administratives, ou bien en dehors du SAIVAJ et affecter indirectement les services.

En fonction des situations, ces événements pourront donner lieu à des situations de crise, être gérés directement au niveau des autorités qualifiées locales ou zonales, des directions, des autorités qualifiées des opérateurs d'importance vitale, ou même nécessiter la mise en œuvre d'une coordination ministérielle ou interministérielle.

### 7.2.3 Remontée rapide systématique de l'information auprès du haut fonctionnaire de défense et de sécurité

L'évolution toujours possible des situations vers une coordination ministérielle ou interministérielle, la prégnance des problématiques de communication - interne, interministérielle ou institutionnelle - rendent indispensable une circulation fluide de l'information, centralisée au sein du SAIVAJ par le secrétaire général du ministère de la justice, haut fonctionnaire de défense et de sécurité.

Plusieurs réseaux organisent la remontée rapide et systématique au secrétaire général des informations relatives à la survenance d'événements de sécurité ou à la gestion de la crise et constituent les vecteurs structurels de circulation de l'information de défense et de sécurité, dans le sens ascendant et descendant :
– au niveau des zones de défense et de sécurité, le réseau des secrétaires généraux – délégués zonaux à la défense et à la sécurité des cours d'appel de zone de défense et de sécurité (CAZDS) ;
– au niveau de l'administration centrale, le réseau des chefs de cabinet (bureau du cabinet GDS, SG, IGSJ, DACG, DACS, DSJ, DAP, DPJJ, SGA et DDS du Conseil d'État) ;
– au niveau du secrétariat général, le réseau des chefs de service (SDAC, SAEI, SADJAV), des sous-directeurs et du chef du département de l'information et de la communication.

Le chef de cabinet du secrétaire général, responsable de leur animation, centralise les informations et les rediffuse en tant que de besoin ; il assure une liaison constante avec le cabinet du garde des sceaux.

#### 7.2.3.1 Réseau des secrétaires généraux des cours d'appel sièges de zones de défense et de sécurité

Les secrétaires généraux auprès des chefs de cour de zone de défense et de sécurité assument de manière permanente la continuité des fonctions de délégué zonal à la défense et à la sécurité (DZDS) ; ils animent le réseau zonal des délégués à la défense et à la sécurité qui constitue le réseau d'alerte et de gestion de crise du SAIVAJ dans le cadre de la zone de défense et de sécurité :

- secrétaires généraux des cours d'appel ;
- chefs des départements « sécurité et détention » des directions interrégionales des services pénitentiaires ;
- adjoints des directeurs interrégionaux de la protection judiciaire de la jeunesse ;
- coordonnateurs des plates-formes interrégionales du ministère de la justice ;
- présidents des juridictions administratives correspondants des chefs de cour d'appel de zone de défense et de sécurité ou leurs délégués.

***Les tableaux qui suivent sont tenus à jour sur le site de la cellule d'appui du HFDS.***

| Réseau des secrétaires généraux des cours d'appel<br>sièges de Zones de défense et de sécurité | | |
|---|---|---|
| **Cabinet du secrétaire général – haut fonctionnaire de défense et de sécurité**<br>Chef de cabinet : Mme Brigitte PASTOURET<br>Tel : 01 44 77 25 93 ; brigitte.pastouret@justice.gouv.fr | | |
| **Cellule d'appui du haut fonctionnaire de défense et de sécurité**<br>HFDSA : M. Gerald BARTHOLOMEW<br>Tel : 01 44 77 89 67 ; gerald.bartholomew@justice.gouv.fr<br>FSSI : M. Stéphane DUBREUIL<br>Tel : 01 44 77 72 33 ; stéphane.dubreuil@justice.gouv.fr | | |
| **Zone de défense et de sécurité** | **Secrétaire général Première présidence** | **Secrétaire général Parquet général** |
| **DOUAI** | M. Paul BARINCOU<br>Tel : 03 27 93 28 53<br>paul.barincou@justice.fr | M. Damien LEVADOU<br>Tel : 03 27 93 28 73<br>damien.levadou@justice.fr |
| **PARIS** | M. Pascal LE LUONG<br>Tel : 01 44 32 66 58<br>paul.le-luong@justice.fr | Mme véronique ANDRIOLLO<br>Tel : 01 44 32 75 94<br>veronique.andriollo@justice.fr |
| **RENNES** | Mme Marie-Pierre ROLLAND<br>Tel : 02 23 20 44 15<br>marie-pierre.rolland@justice.fr | M. Rodolphe JARRY<br>Tel : 02 23 20 43 12<br>rodolphe.jarry@justice.fr |
| **BORDEAUX** | Mme Laurence-Anne LEGALL-MICHEL<br>Tel : 05 47 33 94 11<br>laurence.legall@justice.fr | Mme Caroline CALBO<br>Tel : 05 47 33 95 16<br>caroline.calbo@justice.fr |
| **Aix-en-Provence** | M. Thierry AZEMA<br>Tel : 04 42 33 80 14<br>thierry.azema@justice.fr | M. Marc HELLIER<br>Tel : 04 42 33 80 62<br>marc.hellier@justice.fr |
| **LYON** | Mme Emmanuele CARDONA<br>Tel : 04 72 77 30 76<br>emmanuele.cardona@justice.fr | M. Jean-Philippe RIVAUD<br>Tel : 04 72 77 30 30<br>jean-philippe.rivaud@justice.fr |
| **COLMAR** | Mme Catherine BRUERE<br>Tel : 03 89 20 89 29<br>Catherine.bruere@justice.fr | Mme Marie-Hélène CALVANO<br>Tel : 03 80 20 89 10<br>marie-helene.calvano@justice.fr |
| **Fort-de-France** | Mme Nathalie DELPEY-CORBAUX<br>Tel : 05 96 48 71 25<br>nathalie.delpey-corbaux@justice.fr | M. Alexandre AUBERT<br>Tel : 05 96 48 71 42<br>alexandre.aubert@justice.fr |
| **Saint-Denis – de-La-Réunion** | Mme Bérangère VALLEE<br>Tel : 02 62 40 58 07<br>marie-therese.rix-geay@justice.fr | N…<br>Tel : 02 62 40 58 00 |
| **NOUMEA** | M. Jean-Michel STOLTZ<br>Tel : 00 687 27 93 90<br>jean-michel.stoltz@justice.fr | Mme Fabienne SAVREUX<br>Tel 00 687 27 93 54<br>fabienne.savreux@justice.fr |
| **PAPEETE** | Mme Isabelle URIOT<br>Tel : 00 689 87 72 40 40<br>isabelle.uriot@justice.fr | M. Bernard SIMIER<br>Tel : 00 689 40 41 55 13<br>bernard.simier@justice.fr |

### 7.2.3.2 Réseau des chefs de cabinet

| Réseau des chefs de cabinet | |
|---|---|
| **Ministre de la justice** | Chef de cabinet de la ministre : Mme Anne WURTZ<br>Tel : 01 44 77 61 71 ; anne.wurtz@justice.gouv.fr |
| **Bureau du cabinet** | Chef du bureau de cabinet : M. Christophe BAYARD<br>Tel : 01 44 77 63 10 ; christophe.bayard@justice.gouv.fr |
| **SG - HFDS** | Chef de cabinet : Mme Brigitte PASTOURET<br>Tel : 01 70 22 89 26 ; brigitte.pastouret@justice.gouv.fr<br>Cellule d'appui du haut fonctionnaire de défense et de sécurité<br>Adjoint du HFDS : M. Gerald BARTHOLOMEW<br>Tel : 01 70 22 89 67 ; gerald.bartholomew@justice.gouv.fr<br>FSSI : M. Stéphane DUBREUIL<br>Tel : 01 44 77 72 33 ; stephane.dubreuil@justice.gouv.fr |
| **IGSJ** | Inspectrice secrétaire générale de l'IGSJ : Mme Marie-Bénédicte MAIZY<br>Tel : 01 70 22 41 88 ; marie-benedicte.maizy@justice.gouv.fr |
| **DSJ** | Chef de cabinet : M. Arnaud PINSON<br>Tel : 01 70 22 85 25 ; arnaud.pinson@justice.gouv.fr<br>Adjoint : M. Robin MURACCIOLE<br>01 70 22 85 12 . robin.muracciole@justice.gouv.fr |
| **DACG** | Chef de cabinet : M. Nicolas BARRET<br>Tel : 01 44 77 65 56 ; nicolas.barret@justice.gouv.fr<br>Adjointe : Mme Marie-Thérèse COULAMY<br>Tel : 01 44 77 22 70 ; marie-therese.coulamy@justice.gouv.fr |
| **DACS** | Chef de cabinet : Mme Marie LAMBLING<br>Tel : 01 44 77 60 52 ; marie.lambling@justice.gouv.fr<br>Adjoint : M. eric MARTIN-HERSENT<br>Tel : 01 44 77 62 36 ; eric.martin-hersent@justice.gouv.frv |
| **DAP** | Directeur de cabinet : Mme Valérie HAZET<br>Tel : 01 70 22 80 13 valerie.hazet@justice.gouv.fr<br>Chef de cabinet : Mme Vanessa PREMPAIN<br>Tel : 01 70 22 80 01 vanessa.prempain@justice.gouv.fr |
| **DPJJ** | Chef de cabinet : M. Steevens TETU-DUMAS<br>Tel : 01 44 77 74 32 ; steevens.tetu-dumas@justice.gouv.fr<br>Adjointe : Mme Nathalie GIL<br>Tel : 01 44 77 75 34 ; nathalie.gil@justice.gouv.fr |
| **CONSEIL D'ÉTAT** | Secrétaire générale adjointe du Conseil d'État : Mme Natacha CHICOT<br>natacha.chicot@conseil-etat.fr |

### 7.2.3.3 Réseau du secrétariat général

| Réseau du secrétariat général | | |
|---|---|---|
| Chef de cabinet : Mme Brigitte PASTOURET<br>Tel : 01 70 22 89 26 ; brigitte.pastouret@justice.gouv.fr<br>Cellule d'appui du haut fonctionnaire de défense et de sécurité<br>HFDSA : M. Gerald BARTHOLOMEW<br>Tel : 01 70 22 89 67 ; gerald.bartholomew@justice.gouv.fr<br>FSSI : M. Stéphane DUBREUIL<br>Tel : 01 44 77 72 33 ; stephane.dubreuil@justice.gouv.fr | | |
| **SDAC** | Chef du service de l'administration centrale | Mme Corine SINASSAMY<br>Tel 01 70 22 89 34<br>corinne.sinnassamy@justice.gouv.fr |
| **SDAC / DMG** | Chef du département des moyens généraux | M. Christophe CARTIER<br>Tel 01 70 22 73 93<br>christophe.cartier@justice.gouv.fr |
| **SAEI** | Chef du service des affaires européennes et internationales | M. Yves BADORC<br>Tel 01 70 22 88 93<br>eric.badorc@justice.gouv.fr |
| **SADJAV** | Chef du service de l'accès au droit et à la justice et à l'aide aux victimes | M. Thierry PITOIS-ETIENNE<br>Tel 01 44 77 63 22 ; Fax 01 44 77 70 50<br>thierry.pitois-etienne@justice.gouv.fr |
| **SDI** | Sous-directrice de l'immobilier | Mme Marie-Hélène HURTAUD<br>Tel 01 70 22 73 82 ;<br>marie-helene.hurtaud@justice.gouv.fr |
| **SDIT** | Sous-directeur de l'informatique et des télécommunications | M. Marc YOLIN<br>Tel 01 70 22 77 05<br>marc.yolin@justice.gouv.fr |
| **SDSE** | Sous-directeur de la statistique et des études | Mme Christine CHAMBAZ<br>Tel 01 70 22 28 57<br>christine.chambaz@justice.gouv.fr |
| **SDAJGC** | Sous-directeur des affaires juridiques générales et du contentieux | M. Fabrice VERRIELE<br>Tel 01.70 22 78 00<br>patricia.rouault-chalier@justice.gouv.fr |
| **SDRHS** | Sous-directrice de la synthèse des ressources humaines | M. Fabrice THEVAUX<br>Tel 01 70 22 72 21<br>fabrice.thevaux@justice.gouv.fr |

## 7.2.4 Gestion de crise

En situation de crise, sans préjudice des compétences opérationnelles dévolues à l'autorité qualifiée en matière de défense et de sécurité (opérateurs d'importance vitale du SAIVAJ, chefs des services déconcentrés), les réseaux définis (chefs de cabinet, secrétaires généraux de CAZDS, services internes du SG) rendent compte de la situation en temps réel au cabinet du secrétaire général du ministère de la justice.

Sans préjudice des compétences opérationnelles dévolues à l'autorité qualifiée en matière de défense et de sécurité (opérateurs d'importance vitale du SAIVAJ), les chefs des services déconcentrés du ministère de la justice (chefs des cours d'appel, directeurs interrégionaux des services pénitentiaires et de la protection judiciaire de la jeunesse, coordonnateurs des platesformes interrégionales), rendent compte de la situation en temps réel aux chefs de cour d'appel de zone de défense et de sécurité ; les présidents des tribunaux administratifs et des cours administratives d'appel tiennent de la même manière les chefs de cour de zone de défense et de sécurité informés de la situation, parallèlement aux comptes-rendus adressés au Conseil d'État.

### 7.2.5 Organisation du ministère de la justice en cas de convocation par le Premier ministre de la cellule interministérielle de crise

#### 7.2.5.1 Annuaire interministériel de crise

L'annuaire interministériel de crise est tenu par le bureau de veille et d'alerte du SGDSN ; il rassemble les identités des personnes immédiatement mobilisables en situation de crise.
Au titre du ministère de la justice, outre les coordonnées du cabinet du garde des sceaux, il intègre les coordonnées des membres du réseau des chefs de cabinet.
La décision par le Premier ministre de convoquer la cellule interministérielle de crise est notifiée par le ministère de l'intérieur aux personnes suivantes :

- secrétariat général : SG-HFDS, chef de cabinet, HFDSA, FSSI, sous-directeur de l'informatique et des télécommunications, adjoint au sous-directeur ;
- DACG : directeur des affaires criminelles et des grâces, chef de cabinet, sous-directeur de la justice pénale spécialisée.

#### 7.2.5.2 Représentation du ministère de la justice en cellule décision

La représentation du ministère de la justice en cellule de crise est organisée en fonction de la nature de la crise :

- résilience du SAIVAJ : HFDS ;
- action publique et traitement judiciaire des victimes, aide aux victimes : DACG ;
- une représentation conjointe est en général assurée.

#### 7.2.5.3 Rôle du secrétariat général du ministère de la justice

Le cabinet du secrétaire général :

- active la cellule d'appui du HFDS ;
- alerte le réseau des chefs de cabinet, le réseau des chefs de cour de zone de défense et de sécurité ainsi que le réseau du secrétariat général ;
- organise en liaison avec le réseau des chefs de cabinet la représentation du ministère de la justice en cellule « situation » ;
- est destinataire pour information de l'ensemble des flux montants et descendants entre la cellule « situation » et les trois réseaux de communication de crise ;
- élabore avec le concours du représentant du ministère en cellule « décision », en liaison avec les cabinets concernés et le cabinet du ministre, la position ministérielle en cellule « décision » ;
- valide les points de situation établis par les représentants « justice » avant leur transmission au responsable de la synthèse « situation » ;
- valide les éléments de communication proposés par le chef du département de l'information et de la communication avant transmission aux niveaux ministériel et interministériel.

#### 7.2.5.4 Rôle du représentant du HFDS ou de la DACG en cellule « décision » de la CIC

Le représentant du ministre en cellule « décision » :

- coordonne l'activité des représentants du SAIVAJ présents en CIC ;
- est destinataire pour information de l'ensemble des échanges de courriels des cellules « communication » , « situation » et « anticipation » ;
- rédige le compte-rendu de séance de la CIC qui sera adressé aux réseaux des chefs de cabinet, des chefs de cour de zone de défense et de sécurité, et du secrétariat général ;

#### 7.2.5.5 Rôle des délégués du ministère de la justice en cellule « situation »

Les délégués du ministère de la justice en cellule « situation » :

- désignés en priorité parmi les personnels ayant suivi la formation « situation » au ministère de l'intérieur, ils sollicitent les cabinets des directions et l'ensemble des services concernés en vue de collecter les éléments d'information pertinents relatifs à la situation de crise au sein du SAIVAJ ;
- ils assurent l'information transversale de l'ensemble des agents du ministère de la justice présents en CIC ;
- ils élaborent le point de situation relatif aux services de la justice et le transmettent après validation du représentant « justice » de la cellule « décision » au responsable de la cellule « situation » de la CIC.
- ils tiennent le cabinet du secrétaire général-HFDS en copie des correspondances et des comptes-rendus.

#### 7.2.5.6 Rôle des délégués du ministère en cellule « anticipation »

Deux délégués ont été désignés par le ministère de la justice, au titre des deux missions d'importance vitale énumérées à l'alinéa 1 de l'article L. 1142-7 du code de la défense : continuité de l'activité pénale et continuité de l'application des peines.

En cellule « anticipation », ils :

- participent aux travaux de la cellule, en alimentant une réflexion prospective permettant d'anticiper la sortie de crise et de formuler des propositions d'actions à la fonction « décision » ;
- tiennent le représentant du HFDS en cellule « décision » informé des délibérations conduites par leur cellule.

### 7.2.6 Organisation du ministère de la justice en situation de crise interne au ministère

En cas d'événements de sécurité donnant lieu à des situations de crise, les autorités qualifiées locales, zonales ou nationales rendent compte du déclenchement de la crise en utilisant les réseaux de remontée rapide de l'information ; elles disposent de la faculté de solliciter l'escalade du niveau de mobilisation des autorités qualifiées pour la gestion de la crise.

La demande d'escalade des autorités qualifiées des opérateurs d'importance vitale est adressée via le réseau des chefs de cabinet (cf tableau §7.2.3.2).

### 7.2.7 Participation du SAIVAJ aux exercices interministériels

La participation des administrations centrales et des services déconcentrés rattachés au SAIVAJ aux exercices interministériels pilotés par le SGDSN est préparée et organisée sous la conduite du haut

fonctionnaire de défense et de sécurité ; l'organisation mise en place se conforme par principe au schéma défini dans le présent chapitre pour la gestion de crise.

- Cette participation comporte un volet propre au SAIVAJ intégrant trois objectifs principaux :

– mobilisation systématique, en fonction des thèmes d'exercice, des réseaux des chefs de cabinet, des chefs de cour d'appel de zone de défense et de sécurité, ainsi que du secrétariat général ;
– entraînement des services de l'administration centrale et des services déconcentrés à la gestion de crise ;
– prise en compte effective des missions des services permettant de tester des dispositifs pouvant être ultérieurement intégrés à la planification de défense et de sécurité, afin d'améliorer la capacité du SAIVAJ à accomplir ses objectifs de résilience.

## *7.3 Prise en charge des victimes d'actes de terrorisme*

- Texte de référence : circulaire du Premier ministre n° 5853/SG du 13 avril 2016

### 7.3.1 Dispositif en cas d'acte de terrorisme commis sur le territoire national

#### 7.3.1.1 Organisation gouvernementale pour la gestion des crises majeures

- Texte de référence : circulaire du Premier miniqstre n° 5567/SG du 2 janvier 2012 (voir § 7.1)

– la direction politique et stratégique de la crise est assurée conjointement par le Président de la République et le Premier ministre ;
– activation de la cellule interministérielle de crise (CIC) ;
– le préfet de département est le directeur des opérations, chargé d'assurer la cohérence de l'action publique par la coordination de l'ensemble des acteurs publics, privés, associatifs, et des collectivités territoriales ;
– le procureur de la République de Paris, dès lors qu'il décide de retenir sa compétence au regard de la qualification terroriste des faits, assure la direction de la réponse judiciaire.

#### 7.3.1.2 La période de crise

##### *7.3.1.2.1 La cellule interministérielle d'aide aux victimes (CIAV)*

- **Constitution de la CIAV**

– ouverte sur décision du Premier ministre ;
– hébergée par le centre de crise et de soutien (CDCS) du MAE ;
– dirigée par le directeur du CDCS qui assure un lien constant avec le référent victimes du parquet de Paris (constitution de la liste unique des victimes), le Premier ministre, la CIC et les services de l'État ;
– constituée d'équipes pluridisciplinaires et interministérielles sur la base de la demande faite par le directeur : administrations (justice, intérieur, affaires étrangères, affaires sociales et santé), associations conventionnées (INAVEM, FENVAC), fonds de garantie des victimes d'actes de terrorisme et autres infractions (FGTI), représentant national des cellules d'urgence médico-psychologique (CUMP), procureur de la République de Paris ;
– quatre agents de chaque ministère doivent pouvoir être mobilisés dans les quatre heures ;

– mise en alerte parallèle du centre opérationnel de réception et de régulation des urgences sanitaires et sociales (CORRUSS) et de la réserve sanitaire de l'établissement de préparation et de réponse aux urgences sanitaires (EPRUS) pour venir en soutien opérationnel au sein de la CIAV.

- **Missions de la CIAV**

– coordination de l'action interministérielle de l'État dans la prise en charge des victimes ;
– traitement en temps réel des informations relatives au bilan victimaire ;
– information transverse des acteurs de l'aide aux victimes ;
– information des victimes et de leurs familles ; établissement d'un lieu d'accueil unique pour les victimes (Paris : École militaire) ou leurs proches en leur permettant de se signaler, de bénéficier d'un soutien psycho-traumatologique, de fournir les éléments nécessaires *ante-mortem* le cas échéant, de bénéficier d'une présence et d'un accueil auprès des structures de médecine légale ;
– recueil des informations concernant l'identité et l'état des blessés, ainsi que les coordonnées de leurs proches ;
– délégation le cas échéant d'une équipe auprès du préfet territorialement compétent pour assurer l'aide aux victimes en province ;
– veille en relation avec le FGTI à la disponibilité des informations nécessaires au versement aux victimes des premières provisions financières ;
– sollicite le ministère des affaires étrangères, qui assurera le lien avec les autorités étrangères compétentes.

- **Communication**

– coordination de l'information autre que judiciaire des victimes.

#### *7.3.1.2.2 Les premières interventions*

- **Porter secours aux victimes**

– mobilisation immédiate des secours dans le cadre des dispositions des plans d'organisation de la réponse de sécurité civile (ORSEC) ;
– le préfet de département assure la direction des opérations de secours (DOS) ;
– le commandant des opérations de secours (COS) assure la prise en charge médicale des victimes ; les blessés pris en charge sur le site sont traités, identifiés (attribution du numéro unique d'identification national (NF 399) et inscrits sur une liste des victimes avant leur entrée dans la chaîne hospitalière ;
– l'Agence régionale de santé (ARS) assure la coordination de la prise en charge hospitalière des victimes au niveau régional
– alertée par le SAMU, la cellule d'urgence médico-psychologique (CUMP) arme des postes d'urgence médico-psychologique (PUMP) afin de prodiguer des soins immédiats aux victimes et à toutes personnes impliquées dans l'événement ; le psychiatre référent assure en lien avec le SAMU la coordination avec l'ARS
– le recueil de l'identité des victimes est assuré dès la prise en charge des victimes sur le terrain ; quand le recueil n'est pas possible, seul le magistrat référent du parquet de Paris pourra confirmer l'identité. Les informations sont tenues à jour dans le système unique d'identification des victimes ; l'ARS puis le CORRUSS assurent la remontée des informations vers la CIAV.

- **Assurer la sécurisation du site et des intervenants**

– le préfet prend les mesures appropriées et confie au commandant des opérations de police (COP) ou de gendarmerie (COG) la mission d'établir un périmètre de sécurité, de maintenir ou de rétablir l'ordre public, de gérer les flux des secours, d'organiser le cas échéant l'intervention des unités de contre-terrorisme.

- **Accompagner les témoins se trouvant sur les lieux**

– identification des témoins, soins médicaux-psychologiques, communication du numéro de la CIAV.

- **Identifier les personnes blessées ou les témoins ayant quitté » les lieux**

– audition par les services d'enquête, et contact par la CIAV pour s'assurer de leur prise en charge.

- **Prise en charge spécifique des personnes décédées**

– conditions de prise en charge des personnes décédées et organisation des opérations de médecine légale sous la direction du procureur de la République de Paris.

- **Numéros d'information du public et d'appel à témoins et lieu d'accueil physique des victimes**

– n° de la CIAV : information des appelants sur la situation des victimes, recueil du signalement des personnes recherchées et point d'entrée pour les victimes et leurs proches ; la CIAV renvoie les appels ne concernant pas les victimes vers la cellule d'information du public mise en place par le préfet de département ;
– n° d'appel à témoins.

#### *7.3.1.2.3 La phase judiciaire*

- **Direction de l'enquête par le procureur de la République de Paris**

– compétence du procureur de la République local dans un premier temps ;
– compétence du parquet de Paris dès que le procureur de Paris reconnaît sa compétence ; il assure alors la direction de l'enquête judiciaire ;

- **Identification, première prise en charge et accompagnement des victimes**

– le procureur de la République de Paris désigne le magistrat référent victimes qui sera en charge de l'établissement de la liste unique des victimes ; le service de police ou de gendarmerie en charge de la coordination de l'enquête désigne un enquêteur référent victimes en charge du recueil de l'ensemble des renseignements indispensables à la prise en charge des victimes et le cas échéant de leurs proches, et de la transmission de ces éléments à l'autorité judiciaire ;
– l'enquêteur référent, en lien constant avec l'unité d'identification de victimes de catastrophes (UIVC) transmet les identités des personnes identifiées comme victimes au magistrat référent victimes ;
– le commandant des opérations de secours rend le référent victimes du service d'enquête coordinateur destinataire de toutes informations utiles relatives à l'identification des victimes ;
– à partir des informations transmises au magistrat référent victimes, le parquet arrête la liste unique des victimes, qui recense les personnes décédées, ou blessées ayant subi un dommage physique ou psychique directement lié aux actes de terrorisme, les personnes impliquées qui se trouvaient sur le lieu des faits au moment de l'acte et qui ont présenté ultérieurement un dommage physique ou psychique qui y est directement lié ;
– cette liste est évolutive, horodatée, et est communiquée en temps réel à la CIAV ;
– le service enquêteur a accès au système d'information numérique standardisé (SINUS) pour la zone de Paris et aux autres systèmes d'identification des victimes de catastrophe (IVC), conformes aux normes internationales ;
– les annonces de décès incombent aux officiers de police judiciaire (OPJ) et agents de police judiciaire (APJ) placés sous le contrôle de l'enquêteur référent victimes, après accord de l'autorité judiciaire et en liaison avec les autorités administratives locales ;
– l'annonce des décès, si possible par contact personnel, s'accompagne de la communication des coordonnées de la CIAV ; à l'issue de l'annonce des décès aux familles, l'annonce officielle de la

liste consolidée des victimes incombe au procureur de la République de Paris, qui pourra ultérieurement organiser une réunion d'information à destination des victimes et de leurs proches ;

- le suivi des opérations médico-légales s'effectue sous la direction du procureur de la République de Paris et relève de la responsabilité exclusive des services enquêteurs; les corps sont d'abord identifiés sous « X » jusqu'à identification par la commission d'identification, selon un protocole défini au niveau international par INTERPOL, s'appuyant sur les cellules « ante mortem » et « post mortem » ; une procédure accélérée d'identification conforme au protocole IVC INTERPOL peut être mise en œuvre avec l'accord du parquet .
- lorsque la CIAV n'est pas activée, que les faits n'ont lieu que sur un seul point du territoire, le procureur de la République de Paris peut requérir directement l'association d'aide aux victimes ; quand les faits sont intervenus sur plusieurs points du territoire, le ministère de la justice (SG/SADJAV) coordonne l'intervention locale des différentes associations.

#### *7.3.1.2.4 La prise en charge des premiers besoins financiers*

- **Prise en charge des frais d'obsèques**

- prise en charge par le FGTI ; la structure de médecine légale communique au FGTI les coordonnées des établissements de pompe funèbre choisis par les proches des défunts ; le FGTI informe la CIAV et le ministère de la justice de ses diligences et des difficultés rencontrées.

- **Versement de provisions**

- l'information du FGTI est assurée par le procureur de la République de Paris ; le FGTI mobilise une cellule interne et procède à la désignation d'un référent dont les coordonnées sont transmises aux victimes, et verse dans un délai d'un mois à compter de la demande qui lui a été faite une ou plusieurs provisions à la victime ou à ses ayants-droit.

- **Prise en charge des soins**

- l'article 63 de la loi de financement de la sécurité sociale pour 2016 simplifie et améliore cette prise en charge.

- **Indemnisation du préjudice des victimes de terrorisme**

- le FGTI assure la réparation intégrale des dommages résultant d'une atteinte à la personne et verse à toute victime directe ou aux ayants-droit des victimes décédées une réparation forfaitaire au titre du « préjudice exceptionnel spécifique des victimes d'actes de terrorisme » (PESVT) ;
- le FGTI est tenu de présenter à toute victime une offre d'indemnisation dans un délai de trois mois à compter du jour où il reçoit de celle-ci la justification de ses préjudices ;
- les victimes disposent du droit d'action devant le TGI contre le FGTI.

### 7.3.1.3 la période post-crise : le comité interministériel de suivi des victimes (CISV)

- dès la désactivation de la CIAV, le Premier ministre peut décider de mettre en place le CIAV (justice, défense, finances, affaires sociales et santé, parquet de Paris, psychiatre référent des CUMP, office national des anciens combattants et victimes de guerre, FGTI, CNAM, CNMSS, INAVEM, FENVAC, et toute personne utile) ; le Premier ministre peut y mettre fin à tout moment ;
- le CISV est une instance de décision chargée de piloter l'organisation et le fonctionnement du dispositif d'accompagnement post-crise des victimes, qui s'articule autour d'un n° d'appel post-crise et d'un espace d'information et de suivi des victimes, physique ou dématérialisé.

### 7.3.2 Dispositif en cas d'acte de terrorisme commis à l'étranger

#### 7.3.2.1 La période de crise

- Texte de référence : protocole de coopération en date du 13 mars 2013 entre le ministère des affaires étrangères et le ministère de la justice.

– le suivi des actes de terrorisme commis à l'étranger relève de la compétence du parquet de Paris ; en cas d'acte de terrorisme impliquant des victimes de nationalité française, le parquet de Paris informe le CDCS de sa saisine, ainsi que des enquêteurs chargés des investigations et de tout projet de déplacement de magistrats ou d'enquêteurs à l'étranger ;
– le CDCS et le parquet de Paris s'informent de toute demande d'assistance et de coopération formée par l'un ou l'autre ou par l'État étranger, aux fins de constatations, d'examens techniques ou médicaux-légaux à l'étranger.

#### 7.3.2.2 La période de crise : le CDCS

##### *7.3.2.2.1 La liste unique des victimes*

- **Établissement de la liste unique des victimes**

– le CDCS et le parquet de Paris échangent en temps réel toutes informations utiles portées à leur connaissance de nature à permettre l'identification et la localisation des ressortissants français victimes, et celles de leur famille, de leur employeur et de leurs ayants-droit ;
– la liste initiale des victimes de nationalité française est établie par les autorités de l'État du lieu de l'attentat ; elle est adressée à l'ambassade de France qui la vérifie et la complète avant d'adresser une liste unique au MAE ainsi qu'aux autorités judiciaires françaises ;
– en cas d'ouverture d'une enquête judiciaire, le parquet de Paris assure la synthèse des différentes listes et dresse une liste unique des victimes françaises ; en l'absence d'ouverture d'une enquête judiciaire en France, cette synthèse et l'établissement d'une liste unique incombent au MAE.

- **Annonce des décès et communication de la liste unique des victimes**

– l'annonce des décès aux familles résidant en France est effectuée par un OPJ sous l'autorité du parquet de Paris ; si le directeur du CDCS est amené à confirmer le décès d'un ressortissant français à ses proches, il en informe le parquet de Paris ; si la famille réside à l'étranger, l'annonce incombe au consulat de France ;
– l'organisation des rencontres avec les familles de victimes décédées fait l'objet d'une étroite concertation entre le CDCS et le parquet de Paris.

##### *7.3.2.2.2 Cas de coopération*

– Commission d'attentats
– sous l'autorité du directeur de cabinet, le CDCS décide de l'opportunité d'ouvrir une cellule de crise, analyse et diffuse les informations recueillies, assure une liaison permanente avec le poste diplomatique pour coordonner l'assistance consulaire, le secours médical et psychologique, la protection des ressortissants français, assure la coordination interministérielle des actions conduites localement, informe le FGTI et veille à l'information et à l'accompagnement en France des familles des victimes ;
– l'identification des victimes françaises est, sauf difficulté insurmontable, réalisée préalablement à leur rapatriement ; les identifications assurées par un service français de police scientifique et technique sont transmises au parquet de Paris par le CDCS ;
– le CDCS et le parquet de Paris s'informent mutuellement en temps réel des modalités de rapatriement des victimes françaises, des nécessités induites par la procédure judiciaire ; le

ministère de la justice (SG-DADJAV) est tenu informé de l'identité des victimes et des démarches engagées auprès des familles.

- **Prise d'otage(s)**

– à chaque prise d'otage, le CDCS met en œuvre une cellule dédiée chargée d'identifier les familles des victimes et d'établir avec elles un premier contact, de les informer régulièrement, de leur assurer un soutien juridico-administratif et une assistance psychologique.

- **Autres missions du CDCS**

– Le CDCS effectue par ailleurs un travail collaboratif avec les services spécialisés, la coordination des acteurs publics, la mobilisation des associations de soutien aux victimes et un suivi des déclarations de presse ;
– Le CDCS fournit une information régulière du ministère de la justice (SG-SADJAV) et du FGTI ;
– Afin d'assurer le suivi de ces victimes après leur retour en France et mettre à leur disposition de manière pérenne l'aide nécessaire, le CDCS s'est vu confier une mission interministérielle de suivi des victimes de prise d'otage à l'étranger.

#### 7.3.2.3 La période post-crise : le comité interministériel de suivi des victimes(CISV)

(voir dispositif au 1.2)
– le MAE est représenté au sein du CISV ;
– le ministère de la justice pourra décider d'organiser un espace physique ou dématérialisé d'information des victimes, en France ou à l'étranger, si les circonstances le justifient.

### 7.3.3 Organisation du ministère de la justice en cas de convocation par le Premier ministre de la cellule interministérielle d'aide aux victimes

#### 7.3.3.1 Annuaire interministériel de crise

L'annuaire interministériel de crise est tenu par le bureau de veille et d'alerte du SGDSN ; il rassemble les identités des personnes immédiatement mobilisables en situation de crise.

La décision par le Premier ministre de convoquer la cellule interministérielle d'aide aux victimes est notifiée par le directeur de la CIAV aux personnes suivantes :
- secrétariat général : SG-HFDS, chef de cabinet, chef du SADJAV, HFDSA ;
- DACG : directeur DACG, chef de cabinet, sous-directeur des affaires pénales spécialisées.

Par ailleurs, le calendrier des permanences respectives (nom, prénom, n° de tel) est échangé entre le cabinet du secrétariat général du ministère de la justice et la direction de la CIAV.

#### 7.3.3.2 Délégation d'urgence « justice »

Une délégation d'urgence « justice » comprenant quatre personnes est mobilisée dans les quatre heures qui suivent la décision d'ouverture de la CIAV pour rejoindre le CDCS ; elle se compose de la manière suivante :
– le membre du SG – CODIR de permanence hebdomadaire ;
– le membre du SADJAV de permanence (chef du SADJAV ou chef du bureau de l'aide aux victimes et de la politique associative (BAVPA) ou adjoint au chef du bureau) ;
– les deux personnels du ministère de la justice d'astreinte hebdomadaire CIAV.

##### *7.3.3.2.1 Rôle du représentant du SADJAV*

Le memebre du SADJAV de permanence :
- exerce les fonctions de coordinateur de la délégation « justice » au sein de la CIAV ;
- assure en temps réel le lien entre la CIAV et le ministère de la justice (SADJAV – Cabinet du SG) ;
- assure en tant que de besoin le lien entre la CIAV et la cellule déportée de la CIAV ;
- assure le soutien documentaire et logistique des intervenants ;
- effectue la sélection des volontaires appelés à renforcer la délégation « justice » ;
- organise chaque soir une réunion de la délégation « justice » pour faire le point de l'activité de la journée ;
- adresse chaque soir un point de situation au ministère de la justice (cabinet du GDS – cabinet du SG) ;

#### *7.3.3.2.2 Premières missions imparties à la délégation « justice »*

Dès la décision d'ouverture de la cellule interministérielle, et sous la responsabilité du chef de SADJAV et du chef du BAVPA, la délégation « justice » :
- prépare la mise en place fonctionnelle et logistique de la délégation ;
- évalue les besoins en ressources humaines en fonction de l'ampleur de l'acte terroriste et les transmet au cabinet du secrétaire général ;
- procède à la préparation des tableaux prévisionnels d'activité des premiers jours, voire de la première semaine ;
- apporte sa contribution à l'élaboration d'éléments de langage, et de fiches d'information adaptées à l'événement.

### 7.3.3.3 Réservoir de volontaires « justice »

- le réservoir de volontaires « justice » correspond au second cercle d'agents du ministère de la justice qui rejoindront la CIAV, à la suite des premiers membres de la délégation « justice » ; il est composé de personnes issues de l'ensemble des directions du ministère de la justice, et qui ont fait acte de volontariat, sur la base de la fiche de mission « écoutant CIAV » diffusée par le secrétariat général ;
- tous les volontaires participent à une réunion de présentation des missions imparties aux « écoutants CIAV » ainsi qu'à une formation organisée par le SADJAV à l'issue de laquelle un livret contenant les documents de référence leur est distribuée (textes, kit d'accueil de la CIAV, annuaire des contacts utiles…)
- tous les volontaires participent à une formation au logiciel de crise « Crisenet » du CDCS ;
- les volontaires sont reçus en rendez-vous par un psychologue du travail au moment de leur inscription.

Dans les suites immédiates de l'ouverture de la CIAV et en fonction de l'évaluation des besoins en ressources humaines « justice », un appel à mobilisation est lancé soit par le BAVPA soit par la cellule d'urgence afin de connaitre les disponibilités des volontaires CIAV en vue de la préparation des plannings de roulement.

Si l'appel à mobilisation se fait pendant la semaine, une réunion est organisée très rapidement au SADJAV (Millénaire) avec les volontaires disponibles afin de constituer le planning des premiers jours. La prise de fonction à la CIAV peut intervenir rapidement, dans les 12 heures à compter de son activation.

#### *7.3.3.3.1 Vacations des volontaires CIAV*

Les permanences ont une durée d'environ 6 heures soit le matin, soit l'après-midi, soit le soir sur la base horaire suivante : 8h00 – 14h00 ou 14h00 – 20h00 ou 20h00-00h00. Cependant, dans les

premiers jours suivant l'activation de la CIAV, les besoins peuvent dépasser ces amplitudes horaires et s'étendre tout au long de la nuit ; en effet, il est fréquent que la CIAV reste ouverte 24h/24h les 3 ou 4 premiers jours.

#### *7.3.3.3.2 Missions confiées aux volontaires CIAV*

Les volontaires CIAV peuvent être positionnés au sein des différents points de permanence de la CIAV, à savoir :

- au CDCS (Quai d'Orsay) : les agents du ministère de la justice intègrent le pôle de suivi des victimes qui traite des situations individuelles des personnes recherchées, blessées, impliquées ou décédées ; ils ont notamment pour mission de répondre aux appels transférés par la cellule de réponse téléphonique qui concernent des situations individuelles particulières et identifiées, mais également de répondre aux mails. Cette cellule assiste les victimes et leurs familles jusqu'à la mise en sommeil de la CIAV. En principe, le ministère de la justice est chargé du sous-pôle « décédés »;
- au Centre d'accueil des familles : les agents du ministère de la justice (de préférence du SADJAV) intègrent en principe l'espace d'information sur les droits, aux côtés des associations d'aide aux victimes. Il s'agit d'un espace collectif permettant aux familles et aux proches de s'informer sur leurs droits ; ils s'assurent du bon fonctionnement de cet espace ;
- à l'institut médico-légal : Les agents du ministère de la justice positionnés à l'institut médico-légal sont a priori ceux de la cellule d'urgence, en tant qu'agents expérimentés.

Chaque jour, en arrivant sur le lieu de permanence CIAV (CDCS, Centre d'accueil des familles, institut-médico-légal), l'agent de l'équipe « justice » reçoit les consignes sur les actions effectuées par celui qu'il vient relever et ce qu'il y a à faire (passation de consignes de 15 min environ en face à face, ou bien par téléphone ou par main courante pour ceux qui ne sont pas amenés à se croiser physiquement, lors de la prise de poste du matin par exemple).

A chaque sortie de la CIAV, l'agent de la délégation « justice » transmet à son tour les consignes à son successeur ou laisse une main-courante au coordinateur « justice ».

### 7.3.3.4 Organisation du SADJAV en temps d'activation de la CIAV

L'activation de la CIAV a pour conséquence de réduire significativement le nombre d'agents présent au SADJAV, principalement au sein du BAVPA. Une organisation spécifique du service en période de CIAV est donc nécessaire.

#### *7.3.3.4.1 Cellule de soutien du SADJAV*

La cellule de soutien du SADJAV, mise en œuvre pour assister la délégation « justice » de la CIAV, est composée des agents du BAVPA épaulés de volontaires si nécessaire.

La prise de fonction des volontaires à la cellule de soutien fait l'objet d'un délai de prévenance d'au moins 48h ; les permanences ont une durée équivalente à une journée de travail habituelle. La cellule de soutien est physiquement positionnée au ministère de la justice (Millénaire ou Vendôme). Les volontaires sont chargés :

- d'élaborer des outils, des fiches, des documents de synthèse (soutien juridique) ;
- d'assurer, en tant que de besoin, la coordination et la communication des agents « justice » positionnés à la CIAV avec les différentes directions du ministère de la Justice ;
- de soutenir le SADJAV sur toute autre tâche organisationnelle ou logistique.

#### *7.3.3.4.2 Documentation de l'événement*

- Dossier infirmatique dédié

Un dossier informatique dédié est crée sur le réseau du SADJAV. Ce dossier comprendra la fiche récapitulative (voir ci-dessous) ainsi que tous les documents ou mails de référence reçus et envoyés.

- Fiche récapitulative

Une fiche récapitulative concernant l'événement est crée et mise à jour régulièrement, en fonction des informations collectées par la cellule de soutien ; outre un bref rappel des faits, cette fiche contient :

– l'annuaire des contacts utiles pour l'évènement spécifique ;
– la description du dispositif de crise mis en place ;
– le bilan victimaire ;
– les diligences effectuées par le ministère de la justice (SG – SADJAV) ;
– le détail de la prise en charge, de l'accompagnement et de l'ouverture de droits exceptionnels mis en place par les acteurs concernés (INAVEM, FENVAC, CPAM, ONACVG) ; pour faciliter la lisibilité de la fiche, ces informations peuvent faire l'objet d'une annexe (suivi victime par victime) ;
– éventuellement, une partie sur l'indemnisation par le FGTI ;
– la procédure judiciaire ;
– les informations complémentaires/actualités (déplacements politiques, moments de commémorations, décorations…).

#### *7.3.3.4.3 Période post-crise*

Dès l'activation de la CIAV, le SADJAV se prépare au passage de relai sur la prise en charge et l'accompagnement des victimes et de leurs proches qui a lieu à la mise en sommeil de la CIAV.

## *7.4 La mise en œuvre du plan VIGIPIRATE et la transmission des alertes*

### 7.4.1 L'application du plan VIGIPIRATE

- Textes de références :

– Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes VIGIPIRATE n° 650/SGDSN/PSN/PSE du 17 janvier 2014 (non protégé) ;
– Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes VIGIPIRATE n° 10200/SGDSN/PSN/PSE du 17 janvier 2014 (CD) ;

#### 7.4.1.1 Présentation du plan VIGIPIRATE

Le plan VIGIPIRATE repose sur deux documents complémentaires : un document public (n° 650) accessible sur le site www.risques.gouv.fr et un document classifié (n° 10200) destiné aux ministères et aux opérateurs d'importance vitale.

Ce plan comporte deux niveaux :

– « VIGILANCE » : selon l'état de la menace, ce niveau peut être amené à évoluer en « VIGILANCE RENFORCÉE » qui se traduit par la mise en place de mesures spécifiques en fonction des secteurs d'activités ;
– « ALERTE ATTENTAT » ;

Le plan développe des stratégies d'action ainsi que des objectifs de sécurité en fonction des vulnérabilités identifiées au plan national.

Ses modalités de mise en œuvre sont arrêtées au niveau ministériel sur la base de l'évaluation de la menace conduite par le coordonnateur national du renseignement, ainsi que sur les instructions du Premier ministre.

### 7.4.1.2 Diffusion des postures VIGIPIRATE

#### *7.4.1.2.1 Rôle du HFDS*

Le HFDS adresse directement à l'ensemble des autorités chargées de leur mise en œuvre les éléments de posture accompagnés des tableaux récapitulatifs spécifiques aux différents opérateurs :

- au niveau central : DDS de l'administration centrale, directeurs d'administration centrale, sous-directeur de l'informatique et des télécommunications, coordonnateurs des plateformes interrégionales de la justice ;
- au niveau déconcentré : chefs de cour d'appel de zone de défense et de sécurité, chefs de cour d'appel, chefs de juridiction, directeurs interrégionaux des services pénitentiaires, directeurs fonctionnels des services pénitentiaires d'insertion et de probation, chefs d'établissement pénitentiaire, directeurs interrégionaux de la protection judiciaire de la jeunesse, directeurs territoriaux de la protection judiciaire de la jeunesse.

En cas de modification inopinée de la posture VIGIPIRATE, le HFDS diffuse une pré-alerte rapide par le réseau des chefs de cabinet.

#### *7.4.1.2.2 Rôle du Centre opérationnel de la sécurité des systèmes d'information (COSSI)*

En matière de sécurité des systèmes d'information, le COSSI peut prescrire, dans un message adressé à la chaîne d'alerte SSI du HFDS et des OIV, les mesures techniques VIGIPIRATE à mettre en œuvre sans délai pour élever le niveau de vigilance en matière de cybersécurité ; une note de régularisation transite ensuite par le circuit du HFDS.

#### *7.4.1.2.3 Rôle des chefs de cour de zone de défense et de sécurité*

Les chefs de cour de zone de défense et de sécurité coordonnent la mise en œuvre de la posture VIGIPIRATE dans le ressort de la zone de défense et sécurité.

#### *7.4.1.2.4 Rôle du référent VIGIPIRATE départemental*

Dans les départements sièges d'une cour d'appel, les secrétaires généraux assument la fonction de référent VIGIPIRATE du préfet de département pour le ministère de la justice ;dans les autres départements, les chefs de juridiction du chef-lieu du département assument cette fonction, qui est partout assurée par le président du tribunal administratif pour les juridictions administratives.

Ces référents, chargés d'animer le réseau des acteurs relevant de leur périmètre pour la mise en œuvre du plan, doivent constituer un appui pour les préfets dans leur démarche de mise en cohérence départementale du dispositif VIGIPIRATE.

Ils rendent compte de leur action auprès des chefs de cour d'appel de zone de défense et de sécurité.

| VIGIPIRATE<br>Correspondants du référent départemental | |
|---|---|
| Autre TGI | Chefs de juridiction |
| Plate-forme interrégionale de la justice | Coordonnateur de la plate-forme |
| DISP | DIA-DISP |
| DSPIP | Directeur fonctionnel du SPIP |
| Établissements pénitentiaires | Chef d'établissement |
| DIPJJ | Adjoint du directeur interrégional |
| DT | Adjoint du directeur territorial |

### 7.4.2 Le tableau des mesures à mettre en œuvre dans le cadre des postures VIGIPIRATE

L'activation permanente du niveau « VIGILANCE » ou « VIGILANCE RENFORCÉE » du plan VIGIPIRATE se traduit au sein des opérateurs du SAIVAJ par la mise en œuvre d'un ensemble de mesures prévues par le plan VIGIPIRATE, et déclinées en fonction de la spécificité des services.

#### 7.4.2.1 Les mesures sont réparties en domaines d'action et en objectifs

Le SAIVAJ est concerné par les domaines d'action et les objectifs suivants :
- domaine d'action « alerte et intervention » / objectif n° 1 : Alerter et communiquer ;
- domaine d'action « alerte et intervention » / objectif n° 2 : Mobiliser et intervenir ;
- domaine d'action « installations et bâtiments » / objectif n° 1 : Adapter la sûreté externe ;
- domaine d'action « installations et bâtiments » / objectif n° 2 : Adapter la sûreté des accès ;
- domaine d'action « installations et bâtiments » / objectif n° 3 : Adapter la sûreté interne ;
- domaine d'action « cybersécurité ».

#### 7.4.2.2 Lecture du tableau de mesures

La première colonne indique le numéro de la mesure et sa nature : mesure définie par le plan national (N) ou déclinaison spécifique à l'opérateur.
La deuxième colonne indique l'éventuelle gradation de la mesure, et son degré de classification.
La troisième colonne indique la catégorie de services responsables de l'application de la mesure.
La quatrième colonne indique l'énoncé de la mesure.

D'autres mesures peuvent être prescrites par le HFDS, en fonction de la nature de la menace. Ces mesures peuvent par ailleurs être adaptées en fonction des priorités locales, sous l'autorité des préfets.

#### 7.4.2.3 Logo VIGIPIRATE

La communication locale et la signalétique à destination des personnels et du public relatives aux mesures VIGIPIRATE mises en œuvre doivent intégrer le nouveau logo « VIGIPIRATE », le logo « ALERTE ATTENTAT » ne devant être utilisé que sur instruction de l'autorité.

#### 7.4.2.4 Tableaux des mesures VIGIPIRATE des opérateurs d'importance vitale

Les mesures inscrites en couleur bleue sont les mesures génériques du plan VIGIPIRATE et les mesures en couleur noire sont les déclinaisons des mesures pour les OIV concernés.

### *7.4.2.4.1 Secrétariat général*

| DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 1<br>ALERTER ET COMMUNIQUER | | | | |
|---|---|---|---|---|
| **N° Mesure** | **Mesure du plan national** | **Nature du service** | **Mesures « secrétariat général »** | **Type de mesure** |
| **ARL 10-01** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | **Tous Services** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | socle |
| **ARL 10-01** | Activer les cellules de veille et d'alerte et les cellules de crise | **Tous Services** | Sur instruction du secrétaire général ou des directeurs d'administration centrale | additionnelle |
| **ARL 11-01** | Diffuser l'alerte au grand public | **Tous Services** | Affichage du logo VIGIPIRATE aux endroits où des mesures de protection sont mises en œuvre | additionnelle |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 2<br>MOBILISER ET INTERVENIR** | | | | |
| **ARL 20-01** | Elaborer et mettre à jour un plan de continuité | **Tous Services** | Elaborer et mettre à jour un plan de continuité | socle |
| **ARL 20-01-02** | | **Tous Services** | Consignes destinées aux prestataires : mettre en place systématiquement des clauses de sécurité dans les contrats | socle |
| **ARL 20-01-04** | | **Tous Services** | Tenue à jour du PPP ou du PP | socle |
| **ARL 20-01-05** | | **Tous Services** | Tenue à jour des annuaires de crise | socle |
| **ARL 20-01-07** | | **Tous Services** | Vidéosurveillance et vidéoprotection, détection par infrarouge et autres matériels de sécurité : maintien des dispositifs électroniques et informatiques en condition opérationnelle ; contrôle régulier et tenue d'un registre de contrôle | socle |
| **ARL 20-01-08** | | **Tous Services** | Lignes spécialisées : contrôle régulier et tenue d'un registre de contrôle | socle |
| **DOMAINE D'ACTION « installations et bâtiments »<br>Objectif n° 1<br>ADAPTER LA SURETE EXTERNE** | | | | |
| **BAT 10-01** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | **Tous Services** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | socle |
| **BAT 10-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle |
| **BAT 10-02** | Surveiller les abords des installations et bâtiments | **Tous Services** | Surveiller les abords des installations et bâtiments | socle |
| **BAT 10-02-02** | | **PIV** | Mise en œuvre d'une vidéosurveillance et d'une vidéoprotection | socle |
| **BAT 10-02-03** | | **PIV** | Port du gilet pare-balles pour les personnels de sécurité | socle |
| **BAT 10-02-04** | | **Tous Services** | Vigilance : compte rendu de tout élément en rapport avec la sécurité | socle |
| **BAT 10-02-05** | | **Tous Services** | Signalement des colis abandonnés à proximité de la structure | socle |

| | | | | |
|---|---|---|---|---|
| **BAT 10-03** | Contrôler les abords des installations et bâtiments | **Tous Services** | Contrôler les abords des installations et bâtiments | socle |
| **BAT 10-03-02** | | **PIV** | Réalisation de rondes périphériques | socle |
| **BAT 10-04** | Confier aux armées des missions de surveillance et d'observation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | socle |
| **BAT 11-02**<br>**BAT 12-02**<br>**BAT 13-02** | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée ; active<br>**Ciblage DR**[5] |
| **BAT 11-03**<br>**BAT 12-03** | Renforcer la surveillance aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée ; active |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 2**<br>**ADAPTER LA SURETE DES ACCES** | | | | |
| **BAT 20-01** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle |
| **BAT 21-01**<br>**BAT 22-01**<br>**BAT 23-01** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle ; graduée |
| **BAT 21-01-02**<br>**BAT 22-01-02**<br>**BAT 23-01-02** | | **PIV** | Dispositifs physiques interdisant l'accès des véhicules | socle ; graduée |
| **BAT 21-01-06**<br>**BAT 22-01-06**<br>**BAT 23-01-06** | | **Tous Services** | Contrôle des personnes extérieures : recueil de l'identité et établissement d'un badge d'accès | additionnelle ; graduée |
| **BAT 21-01-07**<br>**BAT 22-01-07**<br>**BAT 23-01-07** | | **PIV** | Contrôle des personnes extérieures : passage sous le portique de détection | socle ; graduée |
| **BAT 21-01-08**<br>**BAT 22-01-08**<br>**BAT 23-01-08** | | **Tous Services** | Contrôle des personnes extérieures : inspection visuelle ou contrôle des bagages par appareil détecteur | socle ; graduée |
| **BAT 21-01-11**<br>**BAT 22-01-11**<br>**BAT 23-01-11** | | **Tous Services** | Véhicules : contrôle des autorisations d'accès | socle ; graduée |
| **BAT 21-01-15**<br>**BAT 22-01-15**<br>**BAT 23-01-15** | | **Tous Services** | Véhicules : accompagnement des personnes jusqu'à leur prise en charge | socle ; graduée |
| **BAT 21-01-16**<br>**BAT 22-01-16**<br>**BAT 23-01-16** | | **Tous Services** | Colis extérieurs : contrôle des colis extérieurs et du courrier par appareil détecteur ou mode de contrôle adapté | socle ; graduée |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 3**<br>**ADAPTER LA SURETE INTERNE** | | | | |
| **BAT 30-01** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | **Tous Services** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | socle |
| **BAT 30-01-02** | | **Tous Services** | Signalétique appelant à la vigilance destinée à tous les visiteurs extérieurs | socle |
| **BAT 30-01-03** | | **Tous Services** | Contrôle des accès en zone restreinte | socle |
| **BAT 30-01-04** | | **Tous Services** | Vérification de la non-accessibilité des systèmes de ventilation | socle |
| **BAT 30-01-05** | | **Tous** | Dispositif d'alarme dans les | socle |

[5] Il ne doit pas être fait mention du détail, du ciblage et des moyens engagés dans la mise en œuvre des mesures.

| | | | | |
|---|---|---|---|---|
| | | **services** | bureaux d'entretien | |
| **BAT 30-02** | Surveiller la circulation interne des bâtiments et installations | **Tous Services** | Surveiller la circulation interne des bâtiments et installations | socle |
| **BAT 31-01** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | **Tous Services** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | additionnelle graduée ; active |
| **SÉCURITÉ DES SYSTÈMES D'INFORMATION** | | | | |
| **Renforcer la surveillance et le contrôle** | | | | |
| **CYB** | 1.4.1. : Responsabiliser le personnel.<br>1) En rappelant aux utilisateurs les points suivants :<br>- demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens internet y figurant ;<br>- minimiser les navigations vers des sites internet n'ayant pas de rapport avec l'activité professionnelle ;<br>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.<br>2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. | **Tous Services** | ***Idem*** | socle |
| **Protéger logiquement les systèmes d'information** | | | | |
| **CYB** | 4.3. : Protéger logiquement ses systèmes d'information<br>Base documentaire :<br>Notes d'information du site www.cert.ssi.gouv.fr, notamment :<br>- [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ;<br>- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;<br>- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;<br>- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.<br>- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet<br>- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion<br>Guide du site de l'ANSSI, notamment :<br>- [f]www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.<br>- [g] www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques.<br>[a] sécurisation des sites Internet : www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web<br>[b] attaques par défiguration : www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration<br>[c] comprendre et anticiper les attaques en déni de service : www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos<br>[d] conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002<br><br>Notification d'incidents :<br>[e] www.ssi.gouv.fr/agence/contacts/cossicert-fr | **Tous Services** | ***Idem*** | socle |

### *7.4.2.4.2 DSJ*

| **DOMAINE D'ACTION « alerte et intervention »**<br>**Objectif n° 1**<br>**ALERTER ET COMMUNIQUER** |
|---|

| N° Mesure | Mesure du plan national | Nature du service | Mesures « Services judiciaires » | Type de mesure |
|---|---|---|---|---|
| **ARL 10-01** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | **Tous Services** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | socle |
| ***ARL 10-02*** | Activer les cellules de veille et d'alerte et les cellules de crise | **Tous Services** | Sur instruction du secrétaire général ou du directeur des services judiciaires | additionnelle |
| ***ARL 11-02*** | Diffuser l'alerte au grand public | **Tous Services** | Affichage du logo VIGIPIRATE aux endroits où des mesures de protection sont mises en œuvre | additionnelle |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 2<br>MOBILISER ET INTERVENIR** | | | | |
| **ARL 20-01** | Elaborer et mettre à jour un plan de continuité | **Tous Services** | Elaborer et mettre à jour un plan de continuité | socle |
| **ARL 20-01-02** | | **Tous Services** | Consignes destinées aux prestataires : mettre en place systématiquement des clauses de sécurité dans les contrats | socle |
| **ARL 20-01-04** | | **Tous Services** | Tenue à jour du PPP ou du PP | socle |
| **ARL 20-01-05** | | **Tous Services** | Tenue à jour des annuaires de crise | socle |
| **ARL 20-01-07** | | **Tous Services** | Vidéosurveillance et vidéoprotection, détection par infrarouge et autres matériels de sécurité : maintien des dispositifs électroniques et informatiques en condition opérationnelle ; contrôle régulier et tenue d'une registre de contrôle | socle |
| **ARL 20-01-08** | | **Tous Services** | Lignes spécialisées : contrôle régulier et tenue d'un registre de contrôle | socle |
| **DOMAINE D'ACTION « installations et bâtiments »<br>Objectif n° 1<br>ADAPTER LA SURETE EXTERNE** | | | | |
| **BAT 10-01** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | **Tous Services** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | socle |
| **BAT 10-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle |
| **BAT 10-02** | Surveiller les abords des installations et bâtiments | **Tous Services** | Surveiller les abords des installations et bâtiments | socle |
| **BAT 10-02-02** | | **PIV** | Mise en œuvre d'une vidéosurveillance et d'une vidéoprotection | socle |
| **BAT 10-02-03** | | **PIV** | Port du gilet pare-balles pour les personnels de sécurité | socle |
| **BAT 10-02-04** | | **Tous Services** | Vigilance : compte rendu de tout élément en rapport avec la sécurité | socle |
| **BAT 10-02-05** | | **Tous Services** | Signalement des colis abandonnés à proximité de la structure | socle |
| **BAT 10-03** | Contrôler les abords des installations et bâtiments | **Tous Services** | Contrôler les abords des installations et bâtiments | socle |
| **BAT 10-03-02** | | **PIV** | Réalisation de rondes périphériques | socle |
| **BAT 10-04** | Confier aux armées des missions de surveillance et | **Tous** | Appréciation du ministère de | socle |

| | | | | |
|---|---|---|---|---|
| | d'observation aux abords des installations et bâtiments désignés | **Services** | l'intérieur | |
| **BAT 11-02**<br>**BAT 12-02**<br>**BAT 13-02** | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée |
| **BAT 11-03**<br>**BAT 12-03** | Renforcer la surveillance aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée ; active |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 2**<br>**ADAPTER LA SURETE DES ACCES** | | | | |
| **BAT 20-01** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle |
| **BAT 21-01**<br>**BAT 22-01**<br>**BAT 23-01** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle ; graduée |
| **BAT 21-01-02**<br>**BAT 22-01-02**<br>**BAT 23-01-02** | | **PIV** | Dispositifs physiques interdisant l'accès des véhicules | socle ; graduée |
| **BAT 21-01-06**<br>**BAT 22-01-06**<br>**BAT 23-01-06** | | **Tous Services** | Contrôle des personnes extérieures : recueil de l'identité et établissement d'un badge d'accès | additionnelle ; graduée |
| **BAT 21-01-07**<br>**BAT 22-01-07**<br>**BAT 23-01-07** | | **PIV** | Contrôle des personnes extérieures : passage sous le portique de détection et Inspection visuelle des bagages | socle ; graduée |
| **BAT 21-01-08**<br>**BAT 22-01-08**<br>**BAT 23-01-08** | | **Tous Services** | Contrôle des personnes extérieures : inspection visuelle ou contrôle des bagages par appareil détecteur | socle ; graduée |
| **BAT 21-01-11**<br>**BAT 22-01-11**<br>**BAT 23-01-11** | | **Tous Services** | Véhicules : vontrôle des autorisations d'accès | socle ; |
| **BAT 21-01-15**<br>**BAT 22-01-15**<br>**BAT 23-01-15** | | **Tous Services** | Véhicules : zccompagnement des personnes jusqu'à leur prise en charge | graduée |
| **BAT 21-01-16**<br>**BAT 22-01-16**<br>**BAT 23-01-16** | | **Tous Services** | Colis extérieurs : vontrôle des colis extérieurs et du courrier par appareil détecteur ou mode de contrôle adapté | socle ; |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 3**<br>**ADAPTER LA SURETE INTERNE** | | | | |
| **BAT 30-01** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | **Tous Services** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | socle |
| **BAT 30-01-02** | | **Tous Services** | Signalétique appelant à la vigilance destinée à tous les visiteurs extérieurs | socle |
| **BAT 30-01-03** | | **Tous Services** | Contrôle des accès en zone restreinte | socle |
| **BAT 30-01-04** | | **Tous Services** | Vérification de la non-accessibilité des systèmes de ventilation | socle |
| **BAT 30-01-05** | | **Tous services** | Dispositif d'alarme dans les bureaux d'entretien | socle |
| **BAT 30-02** | Surveiller la circulation interne des bâtiments et installations | **Tous Services** | Surveiller la circulation interne des bâtiments et installations | socle |
| **BAT 31-01** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | **Tous Services** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | additionnelle ; graduée ; active |

| DOMAINE D'ACTION « rassemblements »<br>OBJECTIF N° 1<br>PROTÉGER LES PERSONNES ET LES FLUX | | | | |
|---|---|---|---|---|
| **RSB 10-01** | Mettre en place un dispositif de surveillance et de contrôle | **Tous Services** | Mettre en place un dispositif de surveillance et de contrôle | socle |
| **RSB 10-01-02** | | **Tous Services** | Police d'audience hors affaires signalées : disposition prévue par les plans de protection | socle |
| **RSB 10-01-03** | | **Tous Services** | Police d'audience (affaires signalées) : disposition prévue par PP et présence de forces de sécurité intérieure | socle |
| **RSB 11-01**<br>**RSB 12-01**<br>**RSB 13-01** | Renforcer la surveillance et le contrôle | **Tous Services** | Renforcer la surveillance et le contrôle | additionnelle ; graduée |
| **SÉCURITÉ DES SYSTÈMES D'INFORMATION** | | | | |
| **Renforcer la surveillance et le contrôle** | | | | |
| **CYB** | 1.4.1. : Responsabiliser le personnel.<br>1) En rappelant aux utilisateurs les points suivants :<br>- demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ;<br>- minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;<br>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.<br>2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. | **Tous Services** | ***Idem*** | socle |
| **Protéger logiquement les systèmes d'information** | | | | |
| **CYB** | 4.3. : Protéger logiquement ses systèmes d'information<br>Base documentaire :<br>Notes d'information du site www.cert.ssi.gouv.fr, notamment :<br>- [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ;<br>- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;<br>- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;<br>- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.<br>- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet<br>- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion<br>Guide du site de l'ANSSI, notamment :<br>-<br>[f]www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.<br>- [g] www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques.<br>[a] sécurisation des sites Internet : www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web<br>[b] attaques par défiguration : www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration<br>[c] comprendre et anticiper les attaques en déni de service : www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos<br>[d] conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002 | **Tous Services** | ***Idem*** | socle |

| | | | | |
|---|---|---|---|---|
| | Notification d'incidents :<br>[e] www.ssi.gouv.fr/agence/contacts/cossicert-fr | | | |

### *7.4.2.4.3 DAP*

| VIGIPIRATE | | | |
|---|---|---|---|
| **N° Mesure** | **Type de mesure et class.** | **Nature du service** | **Mesure** |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 1<br>ALERTER ET COMMUNIQUER** | | | |
| **N ARL 10-01** | Socle | **Tous Services** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement |
| **N ARL 11-01** | Additionnelle | **Tous Services** | Activer les cellules de veille et d'alerte et les cellules de crise |
| **N ARL 11-02** | Socle | **Tous Services** | Affichage du logo VIGIPIRATE aux endroits où des mesures de protection sont mises en œuvre |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 2<br>MOBILISER ET INTERVENIR** | | | |
| **N ARL 20-01** | Socle | **Tous Services** | Elaborer et mettre à jour un plan de continuité |
| **DAP ARL 20-01-02** | Socle | **Tous Services** | Consignes destinées aux prestataires : mettre en place systématiquement des clauses de sécurité dans les contrats |
| **DAP ARL 20-01-03** | Socle | **EP** | Tenue à jour du PPI – Soumettre le PPI au visa de l'autorité préfectorale ; si PIV soumettre le PPP au visa de l'autorité préfectorale –diffuser le PPI (ou le PPP si PIV) aux commandants des forces de sécurité intérieure |
| **DAP ARL 20-01-04** | Socle | **DISP SPIP** | Tenue à jour du PPP ou du PP |
| **DAP ARL 20-01-05** | Socle | **Tous Services** | Tenue à jour des annuaires d'astreinte |
| **DAP ARL 20-01-06** | Socle | **Tous Services** | Tenue à jour des listes de rappel des personnels au repos ou en congés |
| **DAP ARL 20-01-07** | Socle | **Tous Services** | Vidéosurveillance et videoprotection, détection par infrarouge et autres matériels de sécurité : maintien des dispositifs électroniques et informatiques en condition opérationnelle ; contrôle régulier et tenue d'une registre de contrôle |
| **DAP ARL 20-01-08** | Socle | **Tous Services** | Lignes spécialisées : contrôle régulier et tenue d'un registre de contrôle |
| **DOMAINE D'ACTION « installations et bâtiments »<br>Objectif n° 1<br>ADAPTER LA SURETE EXTERNE** | | | |
| **N BAT 10-01** | Socle | **Tous Services** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments |
| **DAP BAT 10-01-02** | Socle | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules |
| **DAP BAT 10-01-03** | Socle | **EP** | Protection par des barrières aménageant l'accès au domaine pénitentiaire, et si possible par la présence d'un glacis clos |
| **N ALR 10-02** | Socle | **Tous Services** | Surveiller les abords des installations et bâtiments |
| **DAP ALR 10-02-02** | Socle | **EP** | Mise en œuvre d'une vidéosurveillance |
| **DAP ALR 10-02-03** | Socle | **EP** | Port du gilet pare-balles |
| **DAP ALR 10-02-04** | Socle | **Tous Services** | Vigilance : compte rendu de tout élément en rapport avec la sécurité |
| **DAP ALR 10-02-05** | Socle | **Tous Services** | Signalement des colis abandonnés à proximité de la structure |
| **N BAT 10-03** | Socle | **Tous Services** | Contrôler les abords des installations et bâtiments |

| | | | |
|---|---|---|---|
| **DAP BAT 10-03-02** | Socle | **EP** | Réalisation de rondes dans le glacis par des agents de l'AP non armés |
| **N BAT 10-04** | Socle | **Tous Services** | Confier aux armées des missions de surveillance et d'observation aux abords des installations et bâtiments désignés |
| **N BAT 11-01 BAT 12-01 BAT 13-01** | Additionnelle graduée **DR** | **Tous Services** | Restreindre voire interdire les activités aux abords des installations et bâtiments désignés |
| **BAT 11-02 N BAT 12-02 BAT 13-02** | Additionnelle graduée **DR** | **Tous Services** | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés |
| **N BAT 11-03 BAT 12-03** | Additionnelle graduée | **Tous Services** | Renforcer la surveillance aux abords des installations et bâtiments désignés |
| **N BAT 13-04** | Additionnelle | **Tous Services** | Confier aux armées la protection d'un nombre limité de sites situés en zone publique |
| **DOMAINE D'ACTION « installations et bâtiments » OBJECTIF N° 2 ADAPTER LA SURETE DES ACCES** | | | |
| **N BAT 20-01** | socle | **Tous Services** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) |
| **N BAT 21-01 BAT 22-01 BAT 23-01** | Socle graduée | **Tous Services** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) |
| **DAP BAT 21-01-02 BAT 22-01-02 BAT 23-01-02** | Socle graduée | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules |
| **DAP BAT 21-01-03 BAT 22-01-03 BAT 23-01-03** | Socle graduée | **Tous Services** | Contrôle des personnels pénitentiaires : Port de la carte professionnelle |
| **DAP BAT 21-01-04 BAT 22-01-04 BAT 23-01-04** | Socle graduée | **EP** | Contrôle des personnels pénitentiaires : Passage sous le portique de détection |
| **DAP BAT 21-01-05 BAT 22-01-05 BAT 23-01-05** | Socle graduée | **EP** | Contrôle des personnels pénitentiaires : Inspection visuelle et contrôle des bagages par appareil détecteur |
| **DAP BAT 21-01-06 BAT 22-01-06 BAT 23-01-06** | Socle graduée | **Tous Services** | Contrôle des personnes extérieures : Recueil de l'identité et établissement d'un badge d'accès |
| **DAP BAT 21-01-07 BAT 22-01-07 BAT 23-01-07** | Socle graduée | **Tous Services** | Contrôle des personnes extérieures : Passage sous le portique de détection |
| **DAP BAT 21-01-08 BAT 22-01-08 BAT 23-01-08** | Socle graduée | **Tous Services** | Contrôle des personnes extérieures : Inspection visuelle et contrôle des bagages par appareil détecteur |
| **DAP BAT 21-01-09 BAT 22-01-09 BAT 23-01-09** | Socle graduée | **EP** | Dépôt des téléphones portables et ordinateurs à la consigne |
| **DAP BAT 21-01-10 BAT 22-01-10 BAT 23-01-10** | Socle graduée | **EP** | Etablissement d'une liste d'autorités autorisées à conserver leur téléphone portable ou leur ordinateur |
| **DAP BAT 21-01-11 BAT 22-01-11 BAT 23-01-11** | Socle graduée | **EP** | Véhicules : Contrôle des autorisations d'accès |
| **DAP BAT 21-01-12 BAT 22-01-12** | Socle graduée | **EP** | Véhicules : Inspection des véhicules |

| | | | |
|---|---|---|---|
| **BAT 23-01-12** | | | |
| **DAP BAT 21-01-13 BAT 22-01-13 BAT 23-01-13** | Socle graduée | **EP** | Véhicules : Passage des personnes embarquées sous le portique de détection |
| **DAP BAT 21-01-14 BAT 22-01-14 BAT 23-01-14** | Socle graduée | **EP** | Véhicules : Inspection visuelle et contrôle des bagages par appareil détecteur |
| **DAP BAT 21-01-15 BAT 22-01-15 BAT 23-01-15** | Socle graduée | **EP** | Véhicules : Accompagnement des personnes jusqu'à leur prise en charge |
| **DAP BAT 21-01-16 BAT 22-01-16 BAT 23-01-16** | Socle graduée | **EP** | Colis extérieurs : Contrôle des colis extérieurs et du courrier par appareil détecteur ou mode de contrôle adapté |
| **DAP BAT 21-01-17 BAT 22-01-17 BAT 23-01-17** | Socle graduée | **EP** | Colis extérieurs : Contrôle au tunnel d'inspection à rayons X et fouille des colis apportés par les familles |
| **DOMAINE D'ACTION « installations et bâtiments » OBJECTIF N° 3 ADAPTER LA SURETE INTERNE** | | | |
| **N BAT 30-01** | Socle | **Tous Services** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès |
| **DAP BAT 30-01-02** | Socle | **Tous Services** | Signalétique appelant à la vigilance destinée à tous les visiteurs extérieurs |
| **DAP BAT 30-01-03** | Socle | **Tous Services** | Contrôle des accès en zone restreinte |
| **DAP BAT 30-01-04** | Socle | **Tous Services** | Vérification de la non-accessibilité des systèmes de ventilation |
| **DAP BAT 30-01-05** | Socle | **SPIP** | Dispositif d'alarme dans les bureaux d'entretien |
| **DAP BAT 30-01-06** | Socle | **SPIP** | Structure sous alarme anti-intrusion |
| **DAP BAT 30-01-07** | Socle | **SPIP** | Système d'interphonie et de vidéo, commande d'ouverture de la porte d'accès |
| **N BAT 30-02** | Socle | **Tous Services** | Surveiller la circulation interne des bâtiments et installations |
| **N BAT 31-01** | Additionnelle graduée | **Tous Services** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) |
| **DAP BAT 31-01-02** | Additionnelle graduée | **EP** | Etablissement d'une liste des personnes extérieures dont la présence est indispensable |
| **DAP BAT 31-01-03** | Additionnelle graduée | **EP** | Suspension provisoire de certaines activités intérieures |
| **DOMAINE D'ACTION « cybersécurité »** | | | |
| **N CYB 42-01 CYB 43-01** | **Socle DR** | **AC** | **Renforcer la protection contre les intrusions dans les systèmes d'information.** |
| **N CYB 42-01-01** | Socle N2 DR | **AC** | Mettre en place l'interface centre opérationnel ministériel ou d'opérateur (COSSIM/O) - COSSI et la vérifier ; transmettre les informations SSI jugées significatives au COSSI |
| **N CYB 42-01-02** | Socle N2 - DR | **AC** | Activer le COSSIM/O aux heures ouvrables et mettre en place les astreintes complémentaires |
| **N CYB 42-01-03** | Socle N2 - DR | **AC** | Rendre compte des impacts (techniques et fonctionnels) des attaques et des mesures prises en conséquence au COSSIM |
| **N CYB 42-01-04** | Socle N2 - DR | **AC** | Transmettre immédiatement au COSSI les informations techniques relatives aux incidents sur les systèmes d'information |
| **N CYB 42-01-05** | Socle N2 - DR | **AC** | Activer les astreintes du personnel affecté à la sécurité des éléments vitaux |
| **N CYB 42-01-06** | Socle N2 - DR | **AC** | Se préparer à activer le plan de continuité de l'activité |

| | | | |
|---|---|---|---|
| **N CYB 42-01-07** | Socle N2 - DR | **AC** | Appliquer sans délai les recommandations de l'ANSSI relatives aux éléments vitaux (dont les recommandations des avis/alertes du CERTA) |
| **N CYB 42-01-08** | Socle N2 - DR | **AC** | Sauvegarder les journaux des éléments vitaux à distance |
| **N CYB 42-01-09** | Socle N2 - DR | **AC** | Adapter à la menace la configuration (fréquence, criticité, taille de sauvegarde) de la journalisation des événements remontés par les éléments vitaux |
| **N CYB 42-01-10** | Socle N2 - DR | **AC** | Adapter et augmenter la fréquence d'analyse des journaux des éléments vitaux |
| **N CYB 42-01-11** | Socle N2 - DR | **AC** | Pour les systèmes d'information concernant les éléments vitaux : adapter le filtrage des fichiers en fonction du signalement (signature, caractéristiques de fichiers spécifiques) ; filtrer certaines sources ou certains groupes de sources ; filtrer certains protocoles de communication ; interdire certains groupes d'utilisateurs |
| **N CYB 42-01-12** | Socle N2 - DR | **AC** | Des équipements de filtrage de niveau réseau (et applicatif) sont pré-déployés en périphérie des sous-réseaux et peuvent être sollicités sans délai |
| **N CYB 42-01-13** | Socle N2 - DR | **AC** | Adapter l'accès interne et vers l'extérieur des systèmes d'information traitant et/ou concernant des éléments vitaux et vulnérables : n'autoriser que certaines sources et destinations ou certains groupes de sources ou de destinations ; n'autoriser que certains protocoles de communication ; n'autoriser que les communications chiffrées ; n'autoriser que certains groupes d'utilisateurs |
| **N CYB 42-01-14** | Socle N2 - DR | **AC** | Interdire l'utilisation de supports amovibles et de solutions mobiles sur des systèmes |
| **N CYB 42-01-15** | Socle N2 - DR | **AC** | Appliquer une configuration système spécifique qui permettrait d'éviter les attaques ou de limiter leurs effets aux postes d'utilisateurs et/ou serveurs |
| **N CYB 42-01-16** | Socle N2 - DR | **AC** | Restreindre la connexion des équipements informatiques infectés aux seuls services permettant le retour à la normale |
| **N CYB 42-01-17** | Socle N2 - DR | **AC** | Isoler d'Internet les systèmes d'information spécifiés |
| **N CYB 42-01-18** | Socle N2 - DR | **AC** | Interdire la connexion d'équipements informatiques nomades aux réseaux internes |
| **N CYB 42-01-19** | Socle N2 - DR | **AC** | Redémarrer ou réinitialiser des services ou des équipements informatiques |
| **N CYB 42-01-20** | Socle N2 - DR | **AC** | Utiliser un réseau déconnecté du réseau usuel pour communiquer en interne et avec le COSSI.Employer les canaux sécurisés à disposition |
| **N CYB 42-01-21** | Socle N2 - DR | **AC** | Mettre en place une sauvegarde régulière de toutes les données critiques. Elever la fréquence de sauvegarde à un niveau permettant la reprise des activités en cas d'altération des données |
| **N CYB 43-01-01** | Socle N3 - DR | **AC** | Activer le COSSIM/O aux heures ouvrables ; mettre en place les astreintes renforcées et s'assurer de leur ralliement sur site en moins d'une heure ; passer en fonctionnement 24h/7j sur demande du COSSI |
| **N CYB 43-01-02** | Socle N3 - DR | **AC** | Activer le COSSIM/O et monter directement à effectif maximal pour assurer un fonctionnement 24h/7j |
| **N CYB 43-01-03** | Socle N3 - DR | **AC** | Activer les astreintes au niveau maximal concernant les éléments vitaux |
| **N CYB 43-01-04** | Socle N3 - DR | **AC** | Appliquer immédiatement les recommandations des avis et alertes du CERTA touchant les éléments vitaux |
| **N CYB 43-01-05** | Socle N3 - DR | **AC** | Activer l'analyse permanente des journaux d'événements des éléments vitaux |
| **N CYB 43-01-06** | Socle N3 - DR | **AC** | Mettre en œuvre tous les moyens nécessaires pour isoler les équipements informatiques externes participant aux attaques en cours |
| **N CYB 43-01-07** | Socle N3 - DR | **AC** | Isoler de tout réseau les équipements informatiques potentiellement infectés |
| **N CYB 43-01-08** | Socle N3 - DR | **AC** | Renouveler les données de connexion des applications affectées par les attaques en cours |
| **N CYB 43-01-09** | Socle N3 - DR | **AC** | Proscrire l'utilisation des protocoles réseau spécifiés |
| **N CYB 43-01-10** | Socle N3 - DR | **AC** | Désactiver et déconnecter physiquement les sources d'alimentation électriques des équipements informatiques spécifiés |
| **N CYB 42-02 CYB 43-02** | **Socle DR** | **AC** | **Renforcer la protection contre les attaques en déni de service.** |
| **N CYB 42-02-01** | Socle N2 - DR | **AC** | Mettre en place l'interface centre opérationnel ministériel ou d'opérateur (COSSIM/O) – COSSI et la vérifier ; transmettre les informations SSI jugées significatives au COSSI |
| **N CYB 42-02-02** | Socle N2 - DR | **AC** | Activer le centre opérationnel ministériel ou d'opérateur (COSSIM/O) aux heures ouvrables et mettre en place les astreintes complémentaires |
| **N CYB 42-02-03** | Socle N2 - DR | **AC** | Rendre compte des impacts (techniques et fonctionnels) des attaques et des mesures prises en conséquence au COSSIM |
| **N CYB 42-02-04** | Socle N2 - DR | **AC** | Transmettre immédiatement au COSSI les informations techniques relatives aux incidents sur les systèmes d'information |
| **N** | Socle | **AC** | Activer les astreintes du personnel affecté à la sécurité des éléments vitaux |

| | | | |
|---|---|---|---|
| **CYB 42-02-05** | N2 - DR | | |
| **N CYB 42-02-06** | Socle N2 - DR | **AC** | Se préparer à activer le plan de continuité d'activité |
| **N CYB 42-02-07** | Socle N2 - DR | **AC** | Modifier la politique de routage et ajouter les systèmes utiles afin de répartir la charge sur plusieurs points d'interconnexion |
| **N CYB 42-02-08** | Socle N2 - DR | **AC** | Transférer l'hébergement des systèmes vers des plateformes capables d'absorber les flux |
| **N CYB 42-02-09** | Socle N2 - DR | **AC** | Filtrer les flux en fonction de leur source/destination et/ou des caractéristiques des paquets qui transitent |
| **N CYB 42-02-10** | Socle N2 - DR | **AC** | Limiter ou réduire le débit en fonction de la source (adresse, port, protocole) |
| **N CYB 42-02-11** | Socle N2 - DR | **AC** | Désactiver les services sinistrés/surchargés (ex : site internet) afin de préserver les services exécutés par le même système informatique (ex : service de messagerie) |
| **N CYB 42-02-12** | Socle N2 - DR | **AC** | S'appuyer sur les opérateurs d'accès à Internet pour qu'ils mettent en place des politiques de filtrage de flux |
| **N CYB 42-02-13** | Socle N2 - DR | **AC** | Mettre en place une sauvegarde régulière de toutes les données critiques. Elever la fréquence de sauvegarde à un niveau permettant la reprise des activités en cas d'altération des données |
| **N CYB 43-02-01** | Socle N3 - DR | **AC** | Activer le COSSIM/O aux heures ouvrables ; mettre en place les astreintes renforcées et s'assurer de leur ralliement sur site en moins d'une heure ; passer en fonctionnement 24h/7j sur demande du COSSI |
| **N CYB 43-02-02** | Socle N3 - DR | **AC** | Activer le COSSIM/O et monter directement à effectif maximal pour assurer un fonctionnement 24h/7j |
| **N CYB 43-02-03** | Socle N3 - DR | **AC** | Modifier ou faire modifier les données de serveurs de noms de domaines afin de rediriger les flux vers une destination inexistante |
| **N CYB 43-02-04** | Socle N3 - DR | **AC** | Etre en mesure d'activer sans délai le plan de continuité de l'activité |
| **N CYB 43-02-05** | Socle N3 - DR | **AC** | Bloquer le trafic concernant une source et/ou une destination (adresse, port, protocole) particulière, avec le soutien de l'opérateur d'accès internet |
| **N CYB 42-03 CYB 43-03** | **Socle N2 / N3 DR** | **AC** | **Renforcer la protection contre une menace sectorielle.** |

### *7.4.2.4.4 DPJJ*

| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 1<br>ALERTER ET COMMUNIQUER** | | | | |
|---|---|---|---|---|
| **N° Mesure** | **Mesure du plan national** | **Nature du service** | **Mesures « Protection judiciaire de la jeunesse »** | **Type de mesure** |
| **ARL 10-01** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | **Tous Services** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | socle |
| ***ARL 10-02*** | Activer les cellules de veille et d'alerte et les cellules de crise | **Tous Services** | Sur instruction du secrétaire général ou du directeur des services judiciaires | additionnelle |
| ***ARL 11-02*** | Diffuser l'alerte au grand public | **Tous Services** | Affichage du logo VIGIPIRATE aux endroits où des mesures de protection sont mises en œuvre | additionnelle |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 2<br>MOBILISER ET INTERVENIR** | | | | |
| **ARL 20-01** | Elaborer et mettre à jour un plan de continuité | **Tous Services** | Elaborer et mettre à jour un plan de continuité | socle |
| **ARL 20-01-02** | | **Tous Services** | Consignes destinées aux prestataires : mettre en place systématiquement des clauses de sécurité dans les contrats | socle |
| **ARL 20-01-04** | | **Tous Services** | Tenue à jour du PPP ou du PP | socle |
| **ARL 20-01-05** | | **Tous Services** | Tenue à jour des annuaires de crise | socle |

| | | | | |
|---|---|---|---|---|
| **ARL 20-01-07** | | **Tous Services** | Vidéosurveillance et vidéoprotection, détection par infrarouge et autres matériels de sécurité : maintien des dispositifs électroniques et informatiques en condition opérationnelle ; contrôle régulier et tenue d'une registre de contrôle | socle |
| **DOMAINE D'ACTION « installations et bâtiments »<br>Objectif n° 1<br>ADAPTER LA SURETE EXTERNE** | | | | |
| **BAT 10-01** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | **Tous Services** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | socle |
| **BAT 10-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle |
| **BAT 10-02** | Surveiller les abords des installations et bâtiments | **Tous Services** | Surveiller les abords des installations et bâtiments | socle |
| **BAT 10-02-02** | | **PIV** | Mise en œuvre d'une vidéosurveillance et d'une vidéoprotection | socle |
| **BAT 10-02-04** | | **Tous Services** | Vigilance : compte rendu de tout élément en rapport avec la sécurité | socle |
| **BAT 10-02-05** | | **Tous Services** | Signalement des colis abandonnés à proximité de la structure | socle |
| **BAT 10-03** | Contrôler les abords des installations et bâtiments | **Tous Services** | Contrôler les abords des installations et bâtiments | socle |
| **BAT 10-04** | Confier aux armées des missions de surveillance et d'observation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | socle |
| **BAT 11-02<br>BAT 12-02<br>BAT 13-02** | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée |
| **BAT 11-03<br>BAT 12-03** | Renforcer la surveillance aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée |
| **DOMAINE D'ACTION « installations et bâtiments »<br>OBJECTIF N° 2<br>ADAPTER LA SURETE DES ACCES** | | | | |
| **BAT 20-01** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle |
| **BAT 21-01<br>BAT 22-01<br>BAT 23-01** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle graduée |
| **BAT 21-01-02<br>BAT 22-01-02<br>BAT 23-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle graduée |
| **BAT 21-01-03<br>BAT 22-01-03<br>BAT 23-01-03** | | **Tous Services** | Contrôle des personnels : Port de la carte professionnelle | socle graduée |
| **BAT 21-01-06<br>BAT 22-01-06<br>BAT 23-01-06** | | **Tous Services** | Contrôle des personnes extérieures : Recueil de l'identité et établissement d'un badge d'accès | additionnelle graduée |
| **BAT 21-01-08<br>BAT 22-01-08<br>BAT 23-01-08** | | **Tous Services** | Contrôle des personnes extérieures : Inspection visuelle ou contrôle des bagages par appareil détecteur (à l'appréciation des directeurs territoriaux) | additionnelle graduée |

| | | | | |
|---|---|---|---|---|
| **BAT 21-01-16**<br>**BAT 22-01-16**<br>**BAT 23-01-16** | | **Tous Services** | Colis extérieurs : Contrôle des colis extérieurs et du courrier par appareil détecteur ou mode de contrôle adapté | socle graduée |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 3**<br>**ADAPTER LA SURETE INTERNE** | | | | |
| **BAT 30-01** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | **Tous Services** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | socle |
| **BAT 30-01-02** | | **Tous Services** | Signalétique appelant à la vigilance destinée à tous les visiteurs extérieurs | socle |
| **BAT 30-01-03** | | **Tous Services** | Contrôle des accès en zone restreinte | socle |
| **BAT 30-01-04** | | **Tous Services** | Vérification de la non-accessibilité des systèmes de ventilation | socle |
| **BAT 30-02** | Surveiller la circulation interne des bâtiments et installations | **Tous Services** | Surveiller la circulation interne des bâtiments et installations | socle |
| **BAT 31-01** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | **Tous Services** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | additionnelle graduée |
| **SÉCURITÉ DES SYSTÈMES D'INFORMATION** | | | | |
| **Renforcer la surveillance et le contrôle** | | | | |
| **CYB** | 1.4.1. : Responsabiliser le personnel.<br>1) En rappelant aux utilisateurs les points suivants :<br>- demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ;<br>- minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;<br>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.<br>2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. | **Tous Services** | ***Idem*** | socle |
| **Protéger logiquement les systèmes d'information** | | | | |
| **CYB** | 4.3. : Protéger logiquement ses systèmes d'information<br>Base documentaire :<br>Notes d'information du site www.cert.ssi.gouv.fr, notamment :<br>- [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ;<br>- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;<br>- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;<br>- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.<br>- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet<br>- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion<br>Guide du site de l'ANSSI, notamment :<br>-<br>[f]www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.<br>- [g] www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques.<br>[a] sécurisation des sites Internet : www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web<br>[b] attaques par défiguration : | **Tous Services** | ***Idem*** | socle |

| | | | | |
|---|---|---|---|---|
| | www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration<br>[c] comprendre et anticiper les attaques en déni de service : www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos<br>[d] conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002<br><br>Notification d'incidents :<br>[e] www.ssi.gouv.fr/agence/contacts/cossicert-fr | | | |

### *7.4.2.4.5 Conseil d'État*

| DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 1<br>ALERTER ET COMMUNIQUER | | | | |
|---|---|---|---|---|
| **N° Mesure** | **Mesure du plan national** | **Nature du service** | **Mesures « Juridictions administratives »** | **Type de mesure** |
| **ARL 10-01** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | **Tous Services** | Disposer d'une chaîne d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement | socle |
| ***ARL 10-02*** | Activer les cellules de veille et d'alerte et les cellules de crise | **Tous Services** | Sur instruction du secrétaire général ou du directeur des services judiciaires | additionnelle |
| ***ARL 11-02*** | Diffuser l'alerte au grand public | **Tous Services** | Affichage du logo VIGIPIRATE aux endroits où des mesures de protection sont mises en œuvre | additionnelle |
| **DOMAINE D'ACTION « alerte et intervention »<br>Objectif n° 2<br>MOBILISER ET INTERVENIR** | | | | |
| **ARL 20-01** | Elaborer et mettre à jour un plan de continuité | **Tous Services** | Elaborer et mettre à jour un plan de continuité | socle |
| **ARL 20-01-02** | | **Tous Services** | Consignes destinées aux prestataires : mettre en place systématiquement des clauses de sécurité dans les contrats | socle |
| **ARL 20-01-04** | | **Tous Services** | Tenue à jour du PPP ou du PP | socle |
| **ARL 20-01-05** | | **Tous Services** | Tenue à jour des annuaires de crise | socle |
| **ARL 20-01-07** | | **Tous Services** | Vidéosurveillance et vidéoprotection, détection par infrarouge et autres matériels de sécurité : maintien des dispositifs électroniques et informatiques en condition opérationnelle ; contrôle régulier et tenue d'une registre de contrôle | socle |
| **DOMAINE D'ACTION « installations et bâtiments »<br>Objectif n° 1<br>ADAPTER LA SURETE EXTERNE** | | | | |
| **BAT 10-01** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | **Tous Services** | Réglementer le stationnement et/ou la circulation aux abords des installations ou bâtiments | socle |
| **BAT 10-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle |
| **BAT 10-02** | Surveiller les abords des installations et bâtiments | **Tous Services** | Surveiller les abords des installations et bâtiments | socle |
| **BAT 10-02-02** | | **Tous** | Mise en œuvre d'une | socle |

| | | | | |
|---|---|---|---|---|
| | | **Services** | vidéosurveillance et d'une vidéoprotection | |
| **BAT 10-02-04** | | **Tous Services** | Vigilance : compte rendu de tout élément en rapport avec la sécurité | socle |
| **BAT 10-02-05** | | **Tous Services** | Signalement des colis abandonnés à proximité de la structure | socle |
| **BAT 10-03** | Contrôler les abords des installations et bâtiments | **Tous Services** | Contrôler les abords des installations et bâtiments | socle |
| **BAT 10-03-02** | | **Tous Services** | Réalisation de rondes périphériques | socle |
| **BAT 10-04** | Confier aux armées des missions de surveillance et d'observation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | socle |
| **BAT 11-02**<br>**BAT 12-02**<br>**BAT 13-02** | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée |
| **BAT 11-03**<br>**BAT 12-03** | Renforcer la surveillance aux abords des installations et bâtiments désignés | **Tous Services** | Appréciation du ministère de l'intérieur | additionnelle graduée |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 2**<br>**ADAPTER LA SURETE DES ACCES** | | | | |
| **BAT 20-01** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle |
| **BAT 21-01**<br>**BAT 22-01**<br>**BAT 23-01** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | **Tous Services** | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | socle graduée |
| **BAT 21-01-02**<br>**BAT 22-01-02**<br>**BAT 23-01-02** | | **Tous Services** | Dispositifs physiques interdisant l'accès des véhicules | socle graduée |
| **BAT 21-01-06**<br>**BAT 22-01-06**<br>**BAT 23-01-06** | | **Tous Services** | Contrôle des personnes extérieures : Recueil de l'identité et établissement d'un badge d'accès | additionnelle graduée |
| **BAT 21-01-07**<br>**BAT 22-01-07**<br>**BAT 23-01-07** | | **Tous Services** | Contrôle des personnes extérieures : Passage sous le portique de détection | socle graduée |
| **BAT 21-01-08**<br>**BAT 22-01-08**<br>**BAT 23-01-08** | | **Tous Services** | Contrôle des personnes extérieures : Inspection visuelle ou contrôle des bagages par appareil détecteur | socle graduée |
| **BAT 21-01-11**<br>**BAT 22-01-11**<br>**BAT 23-01-11** | | **Tous Services** | Véhicules : Contrôle des autorisations d'accès | socle graduée |
| **BAT 21-01-15**<br>**BAT 22-01-15**<br>**BAT 23-01-15** | | **Tous Services** | Véhicules : Accompagnement des personnes jusqu'à leur prise en charge | socle graduée |
| **BAT 21-01-16**<br>**BAT 22-01-16**<br>**BAT 23-01-16** | | **Tous Services** | Colis extérieurs : Contrôle des colis extérieurs et du courrier par appareil détecteur ou mode de contrôle adapté | socle graduée |
| **DOMAINE D'ACTION « installations et bâtiments »**<br>**OBJECTIF N° 3**<br>**ADAPTER LA SURETE INTERNE** | | | | |
| **BAT 30-01** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | **Tous Services** | Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès | socle |
| **BAT 30-01-02** | | **Tous Services** | Signalétique appelant à la vigilance destinée à tous les visiteurs extérieurs | socle |

| | | | | |
|---|---|---|---|---|
| **BAT 30-01-03** | | **Tous Services** | Contrôle des accès en zone restreinte | socle |
| **BAT 30-01-04** | | **Tous Services** | Vérification de la non-accessibilité des systèmes de ventilation | socle |
| **BAT 30-02** | Surveiller la circulation interne des bâtiments et installations | **Tous Services** | Surveiller la circulation interne des bâtiments et installations | socle |
| **BAT 31-01** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | **Tous Services** | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | additionnelle graduée |
| **DOMAINE D'ACTION « rassemblements »<br>OBJECTIF N° 1<br>PROTÉGER LES PERSONNES ET LES FLUX** | | | | |
| **RSB 10-01** | Mettre en place un dispositif de surveillance et de contrôle | **Tous Services** | Mettre en place un dispositif de surveillance et de contrôle | socle |
| **RSB 10-01-02** | | **Tous Services** | Police d'audience hors affaires signalées : disposition prévue par les plans de protection | socle |
| **RSB 10-01-03** | | **Tous Services** | Police d'audience (affaires signalées) : disposition prévue par PP et présence de forces de sécurité intérieure | socle |
| **RSB 11-01<br>RSB 12-01<br>RSB 13-01** | Renforcer la surveillance et le contrôle | **Tous Services** | Renforcer la surveillance et le contrôle | additionnelle graduée |
| **SÉCURITÉ DES SYSTÈMES D'INFORMATION** | | | | |
| **Renforcer la surveillance et le contrôle** | | | | |
| **CYB** | 1.4.1. : Responsabiliser le personnel.<br>1) En rappelant aux utilisateurs les points suivants :<br>- demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ;<br>- minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;<br>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.<br>2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci. | **Tous Services** | ***Idem*** | socle |
| **Protéger logiquement les systèmes d'information** | | | | |
| **CYB** | 4.3. : Protéger logiquement ses systèmes d'information<br>Base documentaire :<br>Notes d'information du site www.cert.ssi.gouv.fr, notamment :<br>- [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ;<br>- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;<br>- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;<br>- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.<br>- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet<br>- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion<br>Guide du site de l'ANSSI, notamment :<br>- [f]www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.<br>- [g] www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques.<br>[a] sécurisation des sites Internet : | **Tous Services** | ***Idem*** | socle |

| | | | | |
|---|---|---|---|---|
| | www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web<br>[b] attaques par défiguration :<br>www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration<br>[c] comprendre et anticiper les attaques en déni de service :<br>www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos<br>[d] conduite à tenir en cas d'intrusion :<br>www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002<br><br>Notification d'incidents :<br>[e] www.ssi.gouv.fr/agence/contacts/cossicert-fr | | | |

### 7.4.3 Remontée rapide de l'information

- Les événements de sécurité liés à l'application du plan VIGIPIRATE feront l'objet d'une remontée rapide de l'information à la diligence des directeurs interrégionaux par la voie hiérarchique ; les directeurs interrégionaux des services pénitentiaires rendent compte de ces événements aux chefs de cour de zone de défense et de sécurité.
- L'information du HFDS est assurée par le chef de cabinet du directeur de l'administration pénitentiaire.

## *7.5 Plans de continuité d'activité*

- Textes de référence :

- article L. 2151-4 du code de la défense
- guide pour réaliser un plan de continuité d'activité (SGDSN – Édition 2013) ;
- circulaire du ministre de la fonction publique du 26 août 2009. Pandémie grippale : gestion des ressources humaines dans la fonction publique (NOR : BCFF0919655C) ;
- –délibération de la CNIL n° 2012-389 du 8 novembre 2012 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en œuvre par les ministères dans le cadre de gestion de crise aux fins de pouvoir mobiliser leurs ressources humaines et celles d'autres structures prestataires de services.

### 7.5.1 Le caractère obligatoire du plan de continuité d'activité

Aux termes de l'article L. 2151-4 du code de la défense, les services désignés opérateurs d'importance vitale sont tenus d'élaborer des plans de continuité ou de rétablissement d'activité.

### 7.5.2 Elaboration des plans de continuité d'activité (PCA)

Le PCA décrit la stratégie de continuité adoptée pour faire face, par ordre de priorité, à des risques identifiés et sériés selon la gravité de leurs effets et leur plausibilité. Il décline cette stratégie en matière de ressources et de procédures documentées qui vont servir de références pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini, lorsque celui-ci a été interrompu à la suite d'une perturbation importante.

- Le contenu du PCA comprend les points suivants, élaborés successivement :

- le contexte ;
- les risques reconnus comme les plus graves ;
- une stratégie de continuité d'activité ;

– la description du rôle des différents responsables ;
– le dispositif de gestion de crise ;
– la maintenance opérationnelle du plan.

- La démarche méthodologique consiste à :

– préciser le contexte et le périmètre ;
– identifier les objectifs et obligations de l'organisation dans le périmètre retenu ;
– formuler des besoins de continuité destinés à faciliter l'atteinte des objectifs et le respect des obligations ;
– identifier, grâce à l'étude des risques, les scénarios de crise qui justifient une démarche de continuité, et définir parmi eux un ordre de priorité ;
– confronter les besoins de continuité aux scénarios retenus ;
– concevoir et formaliser une stratégie de continuité : celle-ci doit résulter de l'optimisation entre d'une part les exigences opérationnelles et leur coût pour respecter les objectifs de continuité, et d'autre part le coût et l'acceptabilité de l'interruption de l'activité ;
– déterminer, dans le cadre de la stratégie, les priorités en matière de ressources et de procédures ;
– définir les rôles des différents responsables pour mettre en œuvre dans les délais prescrits les ressources et les procédures ;
– concevoir et décliner les dispositifs de vérification, de contrôle et d'évolutions régulières du plan.

### 7.5.3 Le service de sécurité nationale

- Textes de référence :

– Articles L. 2151-1 à L. 2151-5 et R. 2151-1 àR. 2151-7 du code de la défense

Le service de sécurité nationale est destiné à assurer la continuité de l'action de l'État, des collectivités territoriales, et des organismes qui leur sont rattachés, ainsi que les entreprises et établissements dont les activités contribuent à la sécurité nationale. Il est applicable au personnel des opérateurs d'importance vitale visés par un plan de continuité ou de rétablissement d'activité.
Sa mise en œuvre, en situation de crise, est décidée par décret en conseil des ministres.
Lors du recours au service de sécurité nationale, les personnes placées sous ce régime, pour tout ou partie du territoire national sont maintenues dans leur emploi habituel ou tenues de le rejoindre.

### 7.5.4 La circulaire du ministre de la fonction publique du 26 août 2009 relative au plan de continuité d'activité « pandémie grippale »

- Le caractère obligatoire du plan de continuité

La circulaire de la Fonction publique rappelle, dans le contexte particulier de la crise de la « grippe A », le caractère obligatoire du plan de continuité de l'activité au sein des services de l'Etat, dans le but de garantir un fonctionnement le plus proche possible des conditions normales en cas de crise grave. Ce plan doit définir les missions prioritaires des services et fixer de manière proportionnée les effectifs pour assurer ces dernières.

- Les plans de continuité des services doivent notamment prévoir de :

– nommer une personne responsable (et un remplaçant) pour coordonner le dispositif de gestion de crise ;

- identifier la liste des postes indispensables au maintien de l'activité ou du service en mode de fonctionnement dégradé et identifier les agents aptes à les occuper ;
- préparer une organisation pour maintenir l'activité ou le service en sécurité, quel que soit le niveau d'absentéisme (postes et tâches indispensables, maintenance, télétravail, *etc*.) ;
- déterminer les différentes dispositions d'aménagement du temps de travail envisageables pour remédier aux éventuelles perturbations liées à l'absentéisme ;
- établir les modalités d'accueil et d'accessibilité à l'établissement, compte tenu des limitations possibles de transport, ainsi que les modalités de restauration collective ;
- recenser les mesures d'hygiène et de sécurité concourant à la protection du personnel et former celui-ci à leur application ;
- informer le personnel sur l'ensemble de ces mesures pour garantir une correcte application des consignes de sécurité et de protection ;
- associer les instances représentatives du personnel, compétentes en matière d'hygiène et de sécurité des conditions de travail (comité technique, comité d'hygiène et de sécurité ou comité d'hygiène, de sécurité et des conditions de travail), à la mise en œuvre de ce dispositif.
-

- Risques à prendre en compte :

Dans le cadre de la présente politique, les risques principaux recensés relèvent :
- du risque de crise sanitaire ;
- du risque de crise informatique ;
- du risque terroriste ou malveillant ;
- du risque naturel (exemple parisien : risque de crue majeure de la Seine) ;
- du risque technologique ou environnemental ;
- des risques accidentels courants (incendie, santé et hygiène, *etc*.) ;
- de tout autre risque identifié par l'autorité hiérarchique.
-

- Niveau d'établissement des plans de continuité :

- opérateurs d'importance vitale ;
- chefs de cour de zone de défense et de sécurité ;
- ensemble des établissements relevant du SAIVAJ.

- Présence des agents :

Il appartient au chef de service de prendre les mesures nécessaires au bon fonctionnement de l'administration et à organiser le service de manière à en assurer la continuité.

La règle générale de fonctionnement du service sera la poursuite de l'activité professionnelle sur le lieu du travail. En fonction des circonstances, il peut être recouru à des solutions de travail à distance, soit dans un service distant du lieu habituel, soit le cas échéant à domicile.

- Constitution d'un annuaire de crise :

Le chef de service établit un annuaire des personnes physiques susceptibles d'assurer les fonctions prioritaires ; cet annuaire constitue un traitement de données à caractère personnel dispensé de déclaration à la CNIL, sous réserve du respect des conditions de la délibération précitée qui sont rappelées en 7.4.5.

Le recueil de ces données permet par ailleurs au service, dans le cadre de l'organisation du travail à distance, de procéder à la constatation du service fait et d'ordonnancer le paiement du traitement de l'agent.

- Sites de desserrement ou de secours

En fonction des risques recensés, le plan de continuité identifie des sites de desserrement ou de secours indispensables à la continuité de l'activité d'importance vitale.

### 7.5.5 Conditions posées par la CNIL

- Finalité du traitement :

– Le traitement doit avoir pour seule finalité, dans le cadre du suivi du PCA, de mobiliser les personnes identifiées par l'organisme. Le traitement ne peut pas être utilisé pour la gestion courante du personnel.

- Personnes concernées par la collecte des données :

– Les agents des administrations de l'État ou d'organismes publics ou privés avec qui la cellule d'appui du HFDS entretient des relations.

- Liste des données concernées par le traitement :

– pour l'identité : nom, nom marital, prénoms, adresses postale et électronique personnelles, coordonnées téléphoniques personnelles ;
– pour la situation familiale : présence au foyer d'enfants à charge de moins de trois ans, présence au foyer d'enfants à charge scolarisés (école maternelle et primaire), autres contraintes personnelles pouvant empêcher de se rendre sur son lieu de travail en cas de crise (exemple : parents à charge). Les données collectées dans cette catégorie doivent se limiter à des réponses par oui ou par non aux questions posées ;
– pour la fonction exercée : lieu de travail, numéro d'identification interne (à l'exclusion du NIR), emploi occupé, caractéristiques du poste, telles que contact avec le public, déplacements fréquents ;
– pour les moyens de déplacement des personnes : mode de transport habituel, mode de transport alternatif, distance lieu de résidence/lieu de travail, permis de conduire.

En tout état de cause, les informations traitées ne doivent pas concerner de données entrant dans le champ des articles 8 et 9 de la loi du 6 janvier 1978 modifiée, c'est-à-dire qu'elles ne doivent pas être relatives aux infractions, condamnations ou mesures de sûreté ni faire apparaître, directement ou indirectement, les origines raciales, les opinions politiques, philosophiques, religieuses, l'appartenance syndicale des personnes ni être relatives à la santé ou à la vie sexuelle de celles-ci.

- La collecte des données a lieu directement auprès des personnes concernées.
- Destinataires des informations :

– peuvent accéder directement aux données relatives au personnel objet du traitement, les agents de la cellule d'appui du HFDS qui sont de permanence ;

– peuvent seules, dans la limite de leurs attributions respectives et en tant que de besoin, être destinataires de tout ou partie des informations, les personnes habilitées des services chargées de la gestion du personnel, et les autres personnes habilitées en charge de la gestion de crise ;

- Durée de conservation :

– les données des personnes visées plus haut peuvent être conservées jusqu'à la cessation définitive de leurs fonctions afférentes aux dispositifs de gestion de crise ;
– elles doivent faire l'objet d'une mise à jour régulière afin de maintenir le caractère opérationnel de l'annuaire de crise ; les données non exactes ou non mises à jour doivent être supprimées en conséquence.

- Information et droits des personnes :

– les personnes concernées par ces traitements sont informées des finalités du traitement, des destinataires des données ainsi que des modalités d'exercice de leurs droits d'accès, de rectification et de suppression lors de la collecte des données. Cette information peut être complétée par une diffusion sur les supports de communication destinés aux agents ;
– le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 ne s'applique pas ;
– les droits d'accès et de rectification s'exercent de manière directe auprès de la cellule d'appui du HFDS ;

- Politique de sécurité et de confidentialité

– des mesures de protection physique et logique doivent être prises afin de préserver la sécurité du traitement et l'intégrité des données traitées ainsi que d'empêcher tout accès ou toute utilisation détournés ou frauduleux de celles-ci, notamment par des tiers non autorisés. Les échanges avec ces destinataires doivent être sécurisés, en particulier concernant les échanges par Internet qui doivent être chiffrés ; le traitement des données doit être en conformité avec les exigences de l'article 34 de la loi du 6 janvier 1978.

### 7.5.6 La politique nationale d'exercices de défense et de sécurité

- Texte de référence :

– instruction interministérielle n° 1210 /SGDSN/PSE/PPS du 15 novembre 2004

La planification de défense et de sécurité englobe les trois volets de la défense : civil, économique et militaire. La politique d'exercices qui lui est associée couvre ces trois domaines et a pour objectif de tester régulièrement les procédures et les mesures prévues par les plans gouvernementaux et ministériels, d'identifier les dysfonctionnements dans les chaînes de gestion de crise et de proposer les modifications appropriées.
Les exercices sont coordonnés par le SGDSN et impliquent tous les échelons de la gestion de crise.

On distingue :
– les exercices antiterroristes, dont le plan de prévention et de protection VIGIPIRATE constitue le socle permanent et qui couvrent les domaines biologique (plan BIOTOX), chimique (plan PIRATOX), nucléaire ou radiologique (plan PIRATOME), maritime (plan PIRATE-MER), aérien (plan PIRATAIR-INTRUSAIR), sécurité des systèmes d'information (plan PIRANET), sécurité des français à l'étranger (plan PIRATE-EXT) ;

– les exercices se rapportant aux problématiques susceptibles d'affecter la continuité d'activité : risques cybernétiques, risques sanitaires, déplacements de population, mouvements sociaux, sûreté nucléaire, gestion des ressources essentielles, aléas climatiques, *etc.* ;
– les exercices en matière de sécurité civile qui relèvent de la responsabilité et de la compétence et de la coordination du ministère de l'intérieur, et qui impliquent les zones de défense et de sécurité et les départements, les services de secours et la population.

## *7.6 Systèmes d'information*

### 7.6.1 Procédures de gestion des incidents

Il est nécessaire de formaliser dans les documents de planification de défense et de sécurité des procédures et des outils de gestion d'incidents des systèmes d'information considérés comme essentiels au SAIV « activités judiciaires ». Ces procédures et outils comprennent notamment :
– un réseau de détection et d'alertes des incidents ;
– l'assurance de la continuité de la sécurité durant toute la durée de l'intervention faisant suite à une alerte ;
– un suivi formel des incidents ;
– la rédaction de fiches réflexes face à des situations d'urgence.

### 7.6.2 Plan de continuité d'activité des systèmes d'information

#### 7.6.2.1 Point de précision sémantique

– PSI (Plan de secours informatique) : couvre tous les aspects de reprise technique en cas d'incident majeur ;
– PRA (Plan de reprise d'activité) : prévoit le volet où les métiers (directions) ont validé l'architecture de reprise et testé le PSI ;
– PCA (Plan de continuité d'activité) : niveau suivant où les aspects hors SI sont pris en compte (salle de crise, téléphonie, mouvement et réinstallation de personnes…).

#### 7.6.2.2 Le plan de continuité d'activité

Le plan de continuité d'activités du système d'information définit les procédures permettant de maintenir les activités critiques pendant et après un désastre (événement majeur ayant des effets sur le long terme).

Tout dossier de sécurité de niveaux 2 ou 3 doit inclure un plan de continuité du système d'information en cas de désastre ou d'interruption. Ce plan s'appuie sur une analyse de risque, qui :

– définit le périmètre physique, fonctionnel et organisationnel du système d'information ;
– décrit les scénarios de risques spécifiques à la continuité des activités en incluant ceux liés à l'externalisation des services ;
– inventorie les fonctions et responsabilités indispensables à la continuité des activités du système d'information ;
– énonce les objectifs de continuité d'activité qui sont déclinés selon trois procédures :
  ▪ les procédures de secours pour assurer une continuité des activités (éventuellement en mode dégradé par des moyens alternatifs et/ou temporaires), pour empêcher l'aggravation du sinistre (par extension géographique ou logique, ou par effet « château de cartes ») et pour supprimer la cause du sinistre ;
  ▪ les procédures de reprise de service nominal du système d'information (le cas échéant graduelle) pour restaurer intégralement les fonctionnalités du système ;

- les procédures d'analyse *a posteriori* et de compensation d'impact.

Le plan de continuité des systèmes d'information doit en sus :

- identifier les risques résiduels exceptionnels générés par son activation ;
- prévoir un volant de personnels suffisant et expérimenté pour palier la vacance, même temporaire, de l'une de ces fonctions ou responsabilités identifiées comme indispensables à la continuité de service. Toute personne remplissant une telle fonction ou responsabilité doit disposer d'un remplaçant de compétences équivalentes et de même niveau de connaissance du SI et des procédures ;
- prévoir des procédures de sauvegarde des informations, des applicatifs et systèmes d'exploitation. Ces procédures doivent être testées régulièrement.

### 7.6.3 Exercices relatifs au plan de continuité des systèmes d'information

Pour un système d'information dont le dossier de sécurité est de niveau 3, le plan de continuité dans son entier doit être testé lors d'un exercice au moins une fois par an.

Pour un système d'information dont le dossier de sécurité est de niveau 2, des exercices de test du plan de continuité sont fortement recommandés.

Pour chaque exercice, il sera constitué un groupe de préparation et de conduite, comprenant des membres de la maîtrise d'ouvrage et de la maîtrise d'œuvre ; les exercices doivent notamment tester les services externalisés. A l'issue de l'exercice, ce groupe rédigera un compte-rendu qui indiquera notamment :

- les dysfonctionnements ou lenteurs observés ;
- les mesures à prendre pour pallier ces dysfonctionnements ou lenteurs ;
- les propositions de mise à jour du plan de continuité.

Dans tous les cas, ce compte-rendu sera adressé à l'autorité qualifiée en matière de sécurité, et au HFDS. Il sera versé au dossier de sécurité.

La gestion de plan de continuité impliquant des partenaires externes doit être prévue, notamment lors de la passation des marchés publics : le contrat doit comporter des éléments relatifs à des exercices réguliers.

## *7.7 Plans de rappel du personnel*

Des plans de rappel des personnels en cas de crise doivent être formalisés au sein des établissements pénitentiaires et de la protection judiciaire de la jeunesse.

Ces plans doivent d'autant plus faire l'objet d'une attention particulière des autorités hiérarchiques que la circonstance qu'une proportion significative de certaines catégories d'agents ait un domicile familial éloigné de l'établissement d'affectation constitue un facteur très prégnant, laissant augurer de difficultés sérieuses pour organiser le ralliement des personnels en situation de crise.

# 8 LIGNE DIRECTRICE N° 6 : DISPOSITIONS RELATIVES AUX RISQUES SANITAIRES

## 8.1.1 Rappel du dispositif du plan national de prévention et de lutte « Pandémie grippale »

- Texte de référence :

– Plan national de prévention et de lutte « pandémie grippale » n° 850 / SGDSN / PSE / PSN d'octobre 2011.

Une pandémie grippale est une épidémie caractérisée par la diffusion rapide et géographiquement très étendue (plusieurs continents ou monde entier) d'un nouveau sous-type de virus résultant d'une transformation génétique conséquente. Le virus possédant des caractéristiques immunologiques nouvelles par rapport aux virus circulant habituellement, l'immunité de la population est faible voire nulle, ce qui a pour conséquence de permettre à la maladie de se propager rapidement.

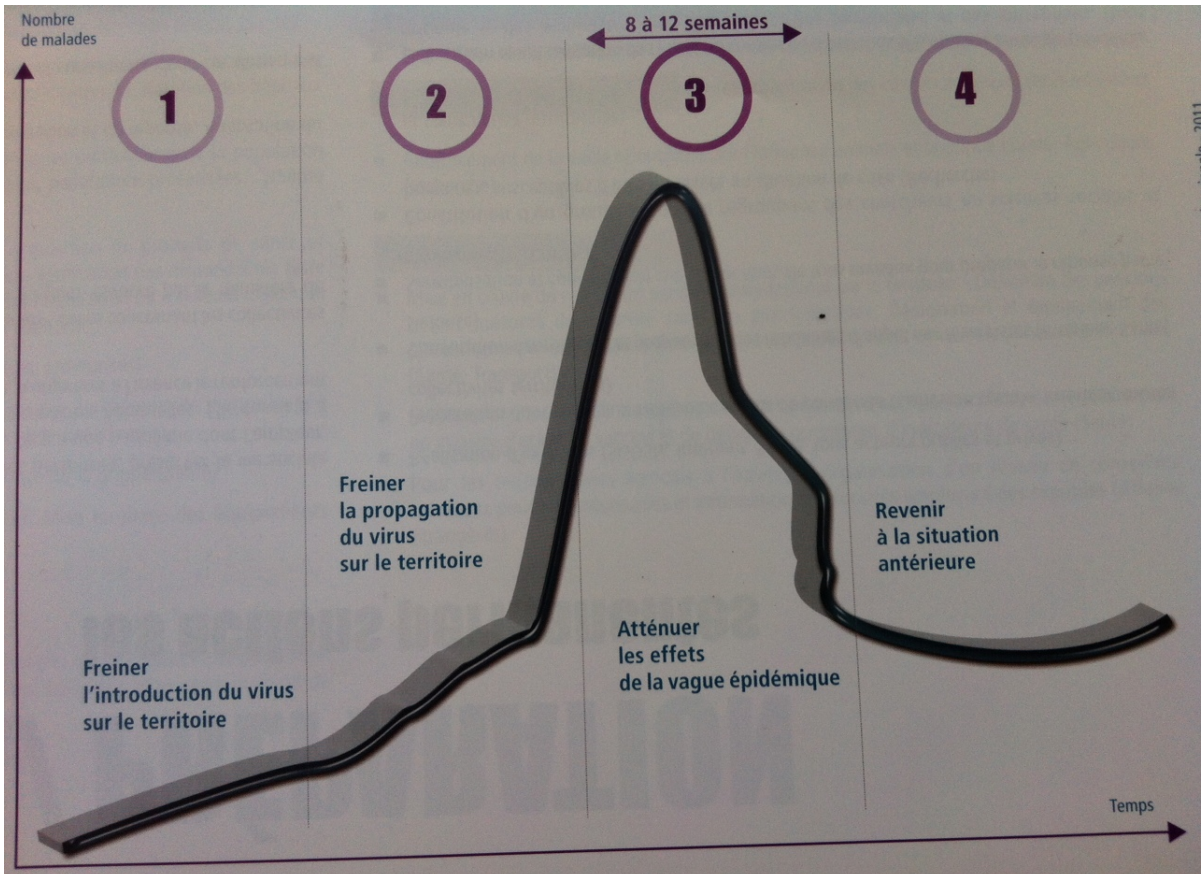
### 8.1.1.1 Phases d'alerte internationale de l'Organisation mondiale de la santé (OMS)

| PHASES OMS | |
|---|---|
| **Période interpandémique OMS** | |
| **Phase 1** | ***Pas de virus grippal circulant chez l'homme*** |
| **Phase 2** | ***Un virus animal, connu pour avoir provoqué des infections chez l'homme, a été identifié sur des animaux sauvages ou domestiques*** |
| **Phase 3** | ***Un virus grippal animal ou hybride animal-humain provoque des infections sporadiques ou de petits foyers chez des humains, sans transmission interhumaine*** |
| **Période d'alerte pandémique (pré-pandémique) OMS** | |
| **Phase 4** | ***Transmission interhumaine efficace*** |
| **Période pandémique** | |
| **Phase 5** | ***Extension géographique de la transmission interhumaine d'un virus grippal animal ou hybride animal-humain*** |
| **Phase 6** | |
| **Fin de vague pandémique OMS** | |
| **Phase 7** | ***- post-pic (fin de vague pandémique) : décroissance du nombre des cas dans la plupart des états, possibilité d'une nouvelle vague pandémique***<br>***- post-pandémique : le nombre de cas correspond à ceux d'une grippe saisonnière*** |

La phase OMS déclarée ne correspond pas obligatoirement à la situation sur le territoire national, la propagation du virus et les vagues pandémiques n'étant pas simultanées sur l'ensemble du globe. La situation peut être aussi très différente entre la métropole et l'outre-mer.

Les limites de la nomenclature de l'OMS ont conduit à définir dorénavant au niveau national 4 stades, traduisant la progression sur le territoire considéré et correspondant à 4 objectifs de conduite de crise pour l'application du plan français.

Ainsi est-il possible de rendre compte de situations différentes en métropole et dans tel ou tel territoire d'outre-mer.
Au-delà de la vague du stade 3, d'autres vagues pandémiques peuvent suivre quelques semaines, quelques mois, voire un, deux ou trois ans plus tard. Elles sont parfois plus graves que la crise initiale.




La plupart des phases peuvent constituer le niveau d'entrée direct dans la crise, sans avoir été précédées par les phases de degré inférieur. A l'inverse, jusqu'en situation de pandémie, un retour à la situation antérieure et à un niveau inférieur est possible. Chacune des phases peut se trouver aggravée par la survenue concomitante d'autres épidémies telles que le SRAS (syndrome respiratoire aiguë sévère) ou une grippe saisonnière.

### 8.1.1.2 Les actions permanentes

La préparation vise à se donner les moyens de protéger les personnes, préserver la vie sociale et économique, puis assurer un retour rapide à la normale face à une pandémie dont l'ampleur, la cinétique et le caractère inattendu peuvent dépasser les capacités habituelles. Elle consiste à élaborer les plans et procédures, à préciser le rôle de chacun, à organiser à l'avance le renforcement en personnels et à se doter des moyens nécessaires.

La planification associe les compétences relevant du Premier ministre (SGDSN) et des différents ministres (agriculture, santé, intérieur, *etc*.) ainsi que des collectivités territoriales.

- Continuité d'activité :

– élaboration et actualisation des plans de continuité d'activité (PCA), avec une annexe « pandémie grippale », définition d'indicateurs de préparation et organisation de circuits de recueil à charge des opérateurs d'importance vitale, mais aussi de l'ensemble des acteurs publics et privés ;
– préparation des mesures et moyens techniques (travail à distance, téléconférences…) à partir du guide du SGDSN.

- Préparation du dispositif de santé :

– ensemble des mesures relevant du ministère de la santé ;
– mesures à charge des opérateurs d'importance vitale, ainsi qu'à l'ensemble des acteurs publics et privés : préparation des stocks de masques, renforcement de la sensibilisation des personnels du réseau santé – hygiène sur la grippe, sensibilisation de l'ensemble des personnels aux règles d'hygiène et mise en place des équipements correspondants.

- Autres dispositifs :

– vaccination ;
– évaluation, recherche et développement ;
– volet international.

### 8.1.1.3 En situation de pandémie

- Organisation de la conduite de crise :

Conformément à la circulaire du Premier ministre n° 5567 en date du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures, la conduite de crise territoriale s'adapte à la nature intersectorielle et interministérielle de la menace. Face à une pandémie très sévère, l'ensemble des acteurs nationaux et locaux sera mobilisé, du citoyen aux services déconcentrés de l'État, aux collectivités territoriales et aux acteurs économiques et sociaux.
La chaîne territoriale des préfets constitue la colonne vertébrale de la préparation et de la conduite de crise. Elle assure la cohérence des mesures et le respect de la stratégie de réponse.

- Stratégie plurisectorielle de réponse :

La stratégie plurisectorielle de réponse a pour objectif de faire face à des pandémies de gravité très diverse. Elle repose sur des mesures dont l'opportunité et la gradation sont à examiner au cas par cas.

– dimension sanitaire : sensibilisation des professionnels de santé, des autres professionnels exposés ainsi que du public au respect des mesures de protection et d'hygiène et mise en place des moyens nécessaires ;
– maintien des activités d'importance vitale en se fondant sur toutes les ressources en personnel disponibles ;
– maintien du respect de l'ordre public et de la loi.

- Stratégie sanitaire qui comporte :

– l'étape de freinage, consistant à retarder l'introduction et la propagation d'une maladie sur le territoire en limitant les transmissions interhumaines ;
– l'étape d'atténuation de l'impact sanitaire, consistant à réduire les effets du virus une fois constatée la circulation active du virus : renforcement des mesures barrières, déploiement de mesures prophylactiques, mise en œuvre de la stratégie vaccinale ;

- la continuité de la vie sociale et économique – solidarité ;
- le maintien pour les opérateurs d'importance vitale, d'un fonctionnement aussi proche que possible des conditions normales, tout en assurant la protection des personnels ;
- la mise en place de plans de continuité d'activité comportant notamment : la désignation du responsable du plan, les méthodes et moyens de protection mis à la disposition des personnels, l'identification des missions prioritaires à assurer en toutes circonstances, l'identification des personnels correspondants dont la présence est indispensable sur le lieu du travail, l'organisation pour le maintien de l'activité y compris en mode dégradé ; le plan doit prévoir plusieurs modes d'organisation selon la sévérité de l'épidémie, et des modalités de travail à distance doivent être prévues ;
- la mobilisation de l'ensemble de la population et la mise en œuvre de solidarités doivent être recherchées ; le strict respect du maintien à domicile, dès lors que l'on est touché par la grippe relève également du devoir de solidarité, pour limiter l'extension de la maladie.

#### 8.1.1.4 Guide d'aide à la décision

Le guide d'aide à la décision permet de se reporter au contexte des principaux stades de l'épidémie :
- Alerte initiale : les premières mesures ;
- Stade 1 : freiner l'introduction du virus sur le territoire ;
- Stade 2 : freiner la propagation du virus sur le territoire ;
- Stade 3 : atténuer les effets de la vague épidémique ;
- Stade 4 : revenir à la situation antérieure et se préparer à une vague suivante éventuelle.

#### 8.1.1.5 Nomenclature des fiches-mesures prévues au plan gouvernemental

(Les mesures préconisées constituent des propositions à examiner au cas par cas et à adapter au contexte si nécessaire)

| NOMENCLATURE DES FICHES-MESURES | |
|---|---|
| **ORGANISATION** | |
| **Demande d'une réunion d'urgence des états-membres de l'UE sur les mesures à prendre au niveau communautaire ; consultation ou information des États membres et de la Commission sur les mesures envisagées par la France.** | **OA1** |
| **Réunion de groupes d'échanges avec les représentants des professions de santé, des associations et tout représentant des secteurs pouvant être touchés par la pandémie.** | **1A2** |
| **Déclenchement de la mobilisation de la recherche en situation d'urgence.** | **1A3** |
| **ÉVALUATION DE LA SITUATION ET ANTICIPATION** | |
| **Évaluation et intégration des informations d'ordre sanitaire.** | **0B1** |
| **Développement des capacités d'anticipation.** | **0B2** |
| **Information par les postes diplomatiques sur la situation et les mesures à l'étranger.** | **0B3** |
| **Organisation de la veille internationale et de la surveillance épidémiologique en pandémie.** | **0B4** |
| **Lancement d'une veille sur la grippe dans les médias (nationaux et internationaux) et sur l'état de l'opinion (incluant Internet et les réseaux sociaux).** | **0B5** |
| **Organisation des laboratoires pour la détection des cas.** | **0B6** |
| **Organisation de la pharmacovigilance.** | **1B7** |
| **Utilisation des tests de diagnostic virologique de confirmation.** | **1B8** |
| **Suivi par les ministères de leurs indicateurs de situations.** | **1B9** |
| **Suivi de situation socio-économique et évaluation des coûts économiques de la pandémie.** | **2B10** |
| **MESURES DESTINÉES AUX VOYAGEURS** | |
| **Information des voyageurs au départ vers les zones affectées et à l'arrivée en provenance des zones** | **0C1** |

| | |
|---|---|
| **affectées.** | |
| **Modalités de mise en œuvre de la surveillance sanitaire et de la prise en charge des cas (suspects et contacts) à l'arrivée aux frontières.** | **0C2** |
| **Modalités de la mise en œuvre de la surveillance sanitaire des voyageurs au départ de France (métropolitaine et/ou outre-mer) et de la prise en charge des cas (suspects et contacts) aux frontières.** | **0C3** |
| **Mesures de circulation et de contrôle sanitaire à mettre en place en cas d'épidémie en métropole aux fins de protéger les collectivités d'outre-mer (vice-versa si la contamination initiale est survenue en outre-mer pour protéger la métropole).** | **0C4** |
| **CONTRÔLE SANITAIRE AUX FRONTIÈRES** | |
| **Contrôle sanitaire au départ des pays touchés en direction de la France.** | **1C5** |
| **MESURES BARRIÈRES** | |
| **Fermeture des crèches, établissements d'enseignement et de formation, internats, accueils collectifs de mineurs.** | **1C6** |
| **Mise en œuvre des mesures visant à limiter la contamination interhumaine (mesures barrières).** | **1C7** |
| **Mesures de protection de populations spécifiques (personnes âgées, personnes handicapées, enfants, personnes sans domicile fixe…) en situation pandémique.** | **2C8** |
| **Encouragement du public à utiliser les moyens de transport individuels. Demande de limitation des déplacements individuels non essentiels.** | **2C9** |
| **Restriction d'activités collectives : spectacles, rencontres sportives, foires et salons, grands rassemblements, limitation des activités cultuelles, limitations d'activités professionnelles, sociales, éducatives et associatives non essentielles.** | **2C10** |
| **Appel à la mise en œuvre de mesures de distance de protection sanitaire : travail à distance, limitation des réunions et des déplacements, téléconférences.** | **2C11** |
| **PRISE EN CHARGE DES CAS ET ORGANISATION DES SOINS** | |
| **Prise en charge médicale des personnes présentant un tableau clinique de grippe (cas suspects ou possibles).** | **0D1** |
| **Prise en charge des personnes ayant eu un contact avec un malade (sujets contacts).** | **0D2** |
| **Investigation autour d'un cas suspect.** | **0D3** |
| **Organisation des soins en période pandémique** | **1D6** |
| **Prise en charge des enfants isolés et des personnes dépendantes non atteintes par la grippe.** | **3D7** |
| **MISE EN PLACE DES STOCKS COMPLEMENTAIRES CONTRE-MESURES MÉDICALES** | |
| **Mesures de sécurisation des établissements de production et de stockage des moyens de protection et produits de santé.** | **0D4** |
| **Acquisition des produits de santé, équipements (hors vaccins et matériels d'injection) et équipements de protection individuelle pour les malades et les sujets contacts.** | **0D5/1** |
| **Distribution des produits de santé et équipements de protection individuelle pour les malades et les sujets contacts.** | **0D5/2** |
| **PROTECTION DES RESSORTISSANTS FRANÇAIS À L'ÉTRANGER** | |
| **Renforcement des stocks de produits de santé et des moyens de protection dans les postes diplomatiques.** | **0E1** |
| **Fermeture des écoles françaises et centres culturels dans les pays touchés.** | **0E2** |
| **Pour le traitement des expatriés, activation d'un réseau de conseillers médicaux grippe et information des sociétés. Si besoin et si possible, envoi d'équipes médicales auprès des postes diplomatiques particulièrement sollicités.** | **0E3** |
| **Prise en charge sur place des ressortissants (cas suspects ou possibles). En fonction des capacités sanitaires locales et de l'état du patient, rapatriement sanitaire possible au cas par cas sur décision conjointe du poste diplomatique, du ministère chargé des affaires étrangères, du ministère chargé de la santé et de l'assureur du malade, sous réserve de garantir la sécurité de l'équipage et de l'équipe d'assistance médicale.** | **0E4** |
| **Recommandation de retour d'expatriés : familles, étudiants français, agents de l'État non indispensables.** | **1E5** |
| **Mise en place d'un dispositif de soutien pour les touristes et ressortissants français non-résidents.** | **1E6** |
| **RESSOURCES HUMAINES POUR LES MISSIONS DE SERVICE PUBLIC** | |
| **Ajustement de la circulaire sur le régime applicable aux agents publics en cas de crise majeure.** | **2F1** |

| | |
|---|---|
| **Modalités de rapprochement, par Pôle emploi, de l'offre et de la demande d'emploi dans certains secteurs jugés prioritaires.** | **3F2** |
| **Mutualisation de ressources en personnels pour les besoins prioritaires : recours aux personnes rendues disponibles par la fermeture d'établissements, aux « jeunes retraités » et étudiants.** | **3F3** |
| **Modalités de renfort en personnels.** | **3F4** |
| **Modalités de renfort en personnels de santé.** | **3F4/1** |
| **Modalités de renfort en personnels dans les domaines non sanitaires.** | **3F4/2** |
| **Montée en puissance de la gendarmerie et de la police nationale.** | **3F4/3** |
| **DÉMARCHE DE SOLIDARITÉ** | |
| **Appel à la solidarité locale (voisinage).** | **3F5** |
| **Recours au bénévolat et aux associations.** | **3F6** |
| **Soutien financier aux foyers touchés par la pandémie** | **3F7** |
| **CONTINUITÉ DE LA VIE SOCIALE ET ÉCONOMIQUE** | |
| **Incitation des administrations, collectivités et opérateurs à mettre en œuvre les plans de continuité d'activité (PCA).** | **3F8** |
| **Activation des solutions permettant d'assurer la continuité pédagogique pour les élèves et étudiants concernés par l'interruption des cours due à une fermeture d'établissement en cas de pandémie.** | **3F9** |
| **Mise à disposition, par tous les ministères et les collectivités territoriales, d'établissements fermés (établissements d'enseignement, centres sportifs, *etc*.) pour satisfaire tous besoins prioritaires.** | **3F10** |
| **Mise en œuvre des dispositions relatives au chômage partiel.** | **3F11** |
| **Mise en sécurité d'installations industrielles à risque.** | **3F12** |
| **Mise en place d'une surveillance des prix et de la disponibilité des produits dans les lieux de distribution.** | **3F13** |
| **Liaisons gouvernementales et chaînes de commandement.** | **3F14** |
| **Maintien des activités essentielles de la défense.** | **3F15** |
| **Production et distribution d'eau potable et contrôle de la qualité des eaux potables et de loisirs.** | **3F16** |
| **Collecte et traitement des déchets ménagers et assimilés (communes, établissements publics de coopération intercommunale et syndicats mixtes).** | **3F17** |
| **Mesures spécifiques relatives au traitement des déchets d'activités de soins à risques infectieux (DASRI).** | **3F18** |
| **Energies, communications électroniques, services financiers et bancaires, services postaux ; mesures économiques et financières y compris mesures douanières.** | **3F19** |
| **Approvisionnement alimentaire et produits de première nécessité : production et distribution.** | **3F20** |
| **Maintien des transports avec rééquilibrage vers les besoins prioritaires planifiés par les services de l'État et les opérateurs concernés.** | **3F21** |
| **Maintien des activités essentielles de Justice.** | **3F22** |
| **Maintien des activités pharmaceutiques, médicales et de produits d'hygiène : produits de santé essentiels.** | **3F23** |
| **Maintien des missions prioritaires de Météo France.** | **3F24** |
| **Plan de continuité des établissements de santé.** | **3F25** |
| **ASSISTANCE À LA POPULATION ET AUX ENTREPRISES** | |
| **Évaluer les populations précarisées par la pandémie.** | **4G1** |
| **Évaluer les entreprises sinistrées. Identifier les activités à relancer en priorité.** | **4G2** |
| **Suivi des procédures d'indemnisation par les compagnies d'assurance.** | **4G3** |
| **Mise en œuvre de mécanismes d'accompagnement de certains secteurs et entreprises mis en difficulté en raison de la pandémie.** | **4G4** |
| **RETOUR D'EXPÉRIENCE ET RÉVISION DES PLANS** | |
| **Demande de retour d'expérience aux administrations, collectivités, entreprises et aux différentes catégories de partenaires associés.** | **4H1** |
| **Révision des plans (plan national, plans ministériels et ensemble des plans dérivés publics et privés).** | **4H2** |
| **COMMUNICATION ET SENSIBILISATION** | |
| **Renforcement de l'information des professionnels de santé sur les mesures sanitaires en matière de pandémie grippale et sur leur rôle dans le dispositif de gestion.** | **0K1** |
| **Renforcement des campagnes de sensibilisation du public aux gestes d'hygiène.** | **1K2** |
| **Activation d'une plateforme ou d'outils d'information du public.** | **1K3** |

| ADAPTATION DU SYSTÈME SANITAIRE ET PRÉPARATION D'UNE VAGUE ÉVENTUELLE | |
|---|---|
| **Détermination de l'opportunité d'une campagne de vaccination.** | **V1** |
| **Acquisition des vaccins et dispositifs d'injection.** | **V2** |
| **Modalités d'organisation d'une campagne de vaccination.** | **V3** |

#### 8.1.1.6 Actions permanentes au niveau gouvernemental

Chaque ministre prend en permanence toutes mesures d'anticipation, de planification et d'organisation afin de garantir l'exécution, durant l'épidémie, des missions prioritaires de son secteur.
À cet effet :

- il s'assure de sa capacité à exécuter les dispositions du plan national et tient à jour son plan de continuité en cas de pandémie, comprenant un volet de protection de la santé ;
- il veille à la préparation et à l'actualisation des plans des établissements publics placés sous sa tutelle, à l'information des opérateurs des secteurs d'activités qui lui sont rattachés et il les incite à préparer des plans de continuité ;
- il prépare les éléments de communication sur les domaines ou pour des publics ciblés ;
- il définit des indicateurs de l'état des ressources critiques et de leur disponibilité lors de la pandémie, ainsi que les chaînes d'information pour les renseigner et les transmettre ;
- il détermine les activités qui nécessiteraient une protection par les forces de sécurité, notamment en cas de troubles à l'ordre public en période pandémique ;
- il prend les dispositions pour que les moyens, matériels et approvisionnements relevant de son secteur de compétence soient disponibles en quantité suffisante et si nécessaire répartis avant le déclenchement du volet pandémique et / ou soient disponibles tout au long de la pandémie.

### 8.1.2 Doctrine nationale de protection des travailleurs face aux maladies hautement pathogènes à transmission respiratoire

- Textes de référence :

- doctrine nationale N° 241/SGDSN/PSE/PSN du 16 mai 2013 ;
- haut conseil de la santé publique, avis du 1er juillet 2011 relatif à la stratégie à adopter concernant le stock État de masques respiratoires.

#### 8.1.2.1 Cadre général de la doctrine

Une maladie infectieuse hautement pathogène à transmission respiratoire est une menace sanitaire majeure à caractère exceptionnel vis-à-vis du strict cadre de la « santé et de la sécurité au travail ».

Face à un tel risque affectant tous les travailleurs, indépendamment de leur statut (salariés, travailleurs indépendants) et de leurs activités, il revient aux pouvoirs publics d'apporter une réponse globale.

La présente doctrine en définit les lignes directrices. Elle est le fruit d'un travail interministériel mené dans un souci d'efficacité et d'économie générale, s'appuyant notamment sur le retour d'expérience acquis lors des pandémies de la décennie écoulée.

Elle constitue le socle de référence commun à partir duquel les ministères pourront établir les directives adaptées à leur secteur de compétence.

*In fine*, la protection des travailleurs relève de la responsabilité des seuls employeurs, publics ou privés. La présente doctrine et ses déclinaisons sectorielles constitueront un guide d'aide à la décision

à leur attention, mais également à celle des travailleurs indépendants, pour la mise en place de mesures de protection adaptées face au caractère exceptionnel d'une pandémie. Il s'agit de répondre de la façon la plus adaptée à une double exigence : l'obligation de protéger le travailleur d'une part, la nécessité d'assurer d'autre part, en fonction de la nature de l'activité et des circonstances, la continuité des activités socio-économiques, en particulier celle des secteurs d'importance vitale.

### 8.1.2.2 Les mesures générales de prévention contre les maladies infectieuses hautement pathogènes à transmission respiratoire

La protection contre les maladies infectieuses hautement pathogènes à transmission respiratoire relève des mesures d'hygiène générale et de mesures complémentaires.

Les mesures d'hygiène sont notamment :
- le lavage régulier des mains ;
- la distance : se tenir, si possible, à une distance de plus d'un mètre d'une autre personne ;
- les règles d'hygiène de base des voies respiratoires ;
- le nettoyage des objets utilisés par le malade.

Les mesures spécifiques sont les écrans et les protections respiratoires. Lors de contacts fréquents et étroits avec des personnes malades ou au statut infectieux inconnu, il est souhaitable, dès que cela est possible, de mettre en place une barrière physique telle qu'un écran ou un masque. Ainsi, il est recommandé aux personnes souffrant d'une maladie infectieuse à transmission respiratoire de porter un masque anti-projection (encore appelé masque chirurgical), même pour des maladies en apparence bénignes.

Chacune de ces mesures, qu'il s'agisse de mesures générales d'hygiène ou de mesures spécifiques, possède une efficacité partielle dans le risque de transmission, le port d'un masque n'étant qu'une mesure de protection parmi d'autres contre les maladies infectieuses hautement pathogènes à transmission respiratoire.

Le respect des mesures d'hygiène générale doit être systématique et fait partie de la promotion et de l'éducation pour la santé.

### 8.1.2.3 La prévention « gouttelette » et « aérosol »

#### *8.1.2.3.1 Les modes de transmission par les gouttelettes et par un aérosol*

Les gouttelettes et les aérosols sont émis par des phénomènes d'expiration, notamment la parole, la toux, les éternuements et lors de procédures médicales telles que l'aspiration trachéo-bronchique.

- Transmission par les gouttelettes :

Dans le cas du virus de l'*influenza*, la transmission s'effectue par de grosses gouttelettes d'un diamètre égal ou supérieur à 5 microns. Les gouttelettes expulsées se retrouvent dans l'environnement immédiat d'une personne exposée. Ces gouttelettes ne demeurent pas en suspension dans l'air et ne voyagent que sur de courtes distances (moins de 1 m). Le maintien d'une distance minimum entre les personnes est une mesure de protection à prendre en compte dans l'analyse de risque.

- Transmission par un aérosol :

La transmission par aérosols consiste en la dissémination d'un agent biologique infectieux par de fines particules en suspension dans l'air. L'Organisation mondiale de la santé (OMS) utilise ce terme pour des particules mesurant moins de 5 microns. La littérature relate des études épidémiologiques suggérant ce mode de transmission, notamment dans les avions et dans les unités de soins.

### *8.1.2.3.2 Les différents types de masques*

Pour être efficace, tout type de masque doit être utilisé dans de bonnes conditions en respectant les règles suivantes :

- consulter les notices d'utilisation fournies par les fabricants ;
- ajuster le masque : dépliage complet, liens bien serrés ou élastiques, couvrir tout le nez et couvrir la bouche, pince-nez ajusté ;
- une fois qu'il est en place, ne pas manipuler le masque car il existe un risque de détérioration de celui-ci et de contamination des mains ;
- se laver les mains après avoir enlevé le masque ;
- éliminer le masque utilisé dans la filière des déchets d'activités de soins à risques infectieux. Il est nécessaire d'organiser cette filière (poubelle de recueil, circuit d'élimination, personnels en charge de cette élimination, *etc*.).

- Le masque anti-projection (ou masque chirurgical) :

Le masque anti-projection est destiné à éviter, lors de l'expiration de celui qui le porte, la projection de sécrétions des voies aériennes supérieures ou de salive pouvant contenir des agents infectieux. Ce masque a pour objectif de protéger l'environnement du porteur.

Le masque anti-projection se présente sous divers formats (ex. bec de canard, plat à plis, coquille pré-moulée) et comporte des cordons ou des élastiques (modèles à coquille pré-moulée) pour les faire tenir en place. Il sert de barrière physique aux gouttelettes qui ont un diamètre de plus de 5 microns de diamètre. Il doit pouvoir retenir des particules à partir d'un micron de diamètre, mais dans les faits, la capacité filtrante de ce type de masque peut varier de 0,5 à plus de 5 microns. Son efficacité à filtrer les gouttelettes est bonne ; en revanche, celle à filtrer les aérosols, dont les particules sont plus fines, est limitée et varie selon les modèles.

Ce type de masque est peu coûteux, confortable, et peut être porté par la grande majorité des individus.

Le masque anti-projection est un dispositif médical. Il bénéficie d'une auto-certification basée sur le système-qualité du fabricant. Les masques anti-projection sont des dispositifs médicaux de classe I relevant de la directive européenne 93/42/CEE (modifiée) du Conseil du 14 juin 1993 relative aux dispositifs médicaux. Ces masques anti-projection sont testés dans le sens de l'expiration notamment avec :

- le test de Green et Vesley : test in vivo. Ce test compare le nombre de bactéries émises par un sujet, avec et sans masque ;
- les tests in vitro de la norme NF EN 14683 de mars 2006 qui spécifient :
- les exigences de construction et de performances ;
- les méthodes d'essai : méthode de détermination *in vitro* de l'efficacité de filtration bactérienne « EFB » (aérosol de bactéries de diamètre moyen de 3 +/- 0,3 µm). Selon le résultat, le masque est classé I (EFB>95%) ou type II (EFB>98%) ; méthode de détermination *in vitro* de la respirabilité.

- L'appareil de protection respiratoire (APR) :

Ce type de masque protège celui qui le porte contre l'inhalation d'aérosols et de sécrétion des voies aériennes supérieures ou de salive présents dans son environnement et pouvant contenir des agents infectieux.

Ces masques, également dénommés anti-particulaires, sont conçus pour filtrer des particules sans avoir subi de transformation pour une utilisation en milieu de soins, mais les résultats de filtration effectués avec un bioaérosol sont comparables à ceux obtenus avec un aérosol de particules inertes.

L'APR est plus coûteux, moins confortable et moins bien supporté par les porteurs que le masque anti-projection. Ce type de masque est un équipement de protection individuelle. Il bénéficie d'une certification CE (Norme EN 149 – 2001).

Ces appareils de protection respiratoire doivent être conformes à la directive 89/686/CEE du 21 décembre 1989 relative aux équipements de protection individuelle comprenant :
- une évaluation de la conformité par des organismes notifiés, au moyen d'essais normalisés décrits dans les normes harmonisées (EN 149 – 2001) ;
- un marquage sur les APR : norme EN et référence datée de la norme, marquage CE et numéro de l'organisme notifié qui réalise le suivi de la fabrication prévu pour les équipements de protection individuelle de catégorie 3, classe d'efficacité : FPP1, FPP2, FPP3 ;
- une notice d'utilisation ;
- une date de péremption.

### 8.1.2.4 L'avis du haut conseil de la santé publique (HCSP)

La direction générale de la santé a saisi le haut conseil de la santé publique sur la stratégie à adopter concernant le stock de masques détenu par l'Etat. Cet avis a été rendu le 1er juillet 2011 et tient compte notamment des retours d'expérience, d'études scientifiques et de quelques études observationnelles sur l'utilisation et l'emploi des différents masques.

Le HCSP propose, pour les salariés régulièrement exposés à des contacts étroits avec le public du fait de leur profession (comme les métiers de guichet) l'utilisation du masque chirurgical sur la base des arguments suivants :
- observance potentiellement supérieure pour le masque anti-projection ;
- pas d'efficacité inférieure démontrée chez les professionnels de santé par rapport à l'appareil de protection respiratoire (APR) dans le contexte de la circulation d'un agent pathogène « courant » ;
- cohérence avec les dispositifs préconisés pour le grand public.

Dans ces conditions, le HCSP privilégie le port de masques chirurgicaux pour les personnels en contact avec le public et les personnes se rendant dans les lieux publics, dès lors que la situation le nécessite. Le HCSP considère que le port du masque FFP2 doit être réservé aux personnels directement exposés à un risque élevé, notamment les personnels de santé exécutant des actes à risque.

### 8.1.2.5 Nouvelle doctrine de protection en fonction de l'exposition aux risques

Le code du travail prévoit les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des salariés. Ces mesures doivent être prises sur la base des principes généraux de prévention, lesquels sont hiérarchisés, le recours à la protection individuelle étant inscrit dans l'avant dernier principe.

Une maladie infectieuse hautement contagieuse à transmission respiratoire sort du cadre strict de « la santé et la sécurité au travail » dans la mesure où l'on a affaire à une menace sanitaire majeure. Face à un tel risque affectant tous les personnels indépendamment de leur statut (salariés, travailleurs indépendants, usagers ou personnes relevant du public) et de leurs activités, il revient aux pouvoirs publics d'apporter une réponse globale.

La situation sanitaire exceptionnelle envisagée et les retours d'expérience des pandémies précédentes amènent à proposer des mesures singulières de protection des travailleurs.

La démarche s'appuie, d'une part, sur les principes généraux de prévention du code du travail incluant l'évaluation des risques et d'autre part, sur la nécessaire cohérence des modalités d'application de mesures exceptionnelles en fonction du caractère continu et inhomogène du risque, ce risque se rencontrant aussi bien au domicile, dans les lieux publics et sur le lieu du travail.

Trois types de mesures de prévention des risques et de protection sont envisagés en fonction des conditions dans lesquelles s'exerce l'activité de travail, depuis la suppression totale de contact jusqu'au port d'un équipement de protection individuelle type FFP2, en passant par la possibilité de mettre en place des dispositions limitant la transmission de la maladie :

- Situation 1 : mesures de suppression du risque de dissémination des agents pathogènes :

a) arrêt de travail lorsque les conditions rendent difficile la mise en place d'autres mesures de protection ;
b) travail à distance (contact par téléphone avec les usagers, *etc*.).

- Situation 2 : mesures de limitation du risque de dissémination des agents pathogènes :

a) distance de sécurité entre les personnes (supérieure à 1 m selon l'OMS) ;
b) écran physique tel qu'un écran anti-agression ;
c) port d'un masque anti-projection (masque chirurgical) par les travailleurs et les usagers à leur contact. Le recours systématique aux masques de protection respiratoire de type FFP2 (EPI) a montré ses limites en matière d'efficacité, car la gêne, voire la difficulté respiratoire liée à leur port, conduit à un faible taux d'utilisation. Le masque anti-projection, en revanche, est mieux supporté en raison d'un confort meilleur, d'une communication verbale plus facile, d'un risque d'irritation cutanée plus réduit et d'une sensation de chaleur plus réduite. Ainsi, l'adhésion au port du masque anti-projection par les travailleurs et par les usagers limite la dissémination des agents pathogènes, chacun protégeant l'autre (fonction altruiste des masques anti-projection).

- Situation 3 : mesures de limitation du risque de transmission de la maladie : mise en place d'une protection individuelle avec le port du masque FFP2 lorsqu'il y a contact étroit sans possibilité de mettre en place une autre mesure :

en situation 2, dès lors qu'aucune mesure de limitation du risque de dissémination des agents pathogènes, parmi celles présentées en situation 2a ou 2b, ne peut être engagée, l'employeur devra prendre les mesures d'organisation nécessaires pour que les travailleurs ne soient en contact qu'avec des personnes auxquelles on aura préalablement distribué des masques anti-projection, et qui les porteront effectivement.

Il revient, *in fine*, à chaque employeur d'examiner, pour les différents postes, de quelles situations ils relèvent et d'évaluer les mesures les plus adaptées.

### 8.1.2.6 Dimensionnement et coût des stocks pour l'employeur

Il revient à chaque employeur de déterminer l'opportunité de constituer des stocks de masques pour protéger son personnel. Le cas échéant, le dimensionnement des stocks est sous-tendu en fonction des éléments suivants :
- la durée prévisible d'une épidémie (une à plusieurs vagues de 8 à 12 semaines, pour la grippe) ;
- la durée d'utilisation d'un masque ;
- le caractère à usage unique des masques ;
- le recensement des tailles de populations cibles ;
- la fourniture gratuite en nombre suffisant ;
- les capacités de fabrication et d'approvisionnement pendant une crise.

Les masques doivent être changés au minimum tous les quatre heures, en fonction des recommandations du fabricant et chaque fois qu'ils deviennent mouillés ou lorsque la personne qui le porte a quitté une zone à haut risque.

Les paramètres de coût sont les suivants :
- acquisition : un masque chirurgical coûte environ dix fois moins cher qu'un masque FFP2 ;
- stockage : le stockage des masques chirurgicaux est largement moins volumineux et donc moins coûteux que celui des masques FFP2, lesquels nécessitent en outre une gestion fine des dates de péremption.

#### 8.1.2.7 Annexes

| Efficacité des appareils de protection respiratoire | | |
|---|---|---|
| **Type de masque** | **Efficacité (%)** | **Fuite totale vers l'intérieur (%)** |
| FFP1 | 78 | 22 |
| FFP2 | 92 | 8 |
| FFP3 | 98 | 2 |

| PRINCIPES GENERAUX DE PREVENTION | |
|---|---|
| **1** | Eviter les risques ; |
| **2** | Evaluer les risques qui ne peuvent être évités ; |
| **3** | Combattre les risques à la source ; |
| **4** | Adapter le travail à l'homme ; |
| **5** | Tenir compte de l'état d'évolution de la technique ; |
| **6** | Remplacer ce qui est dangereux par ce qui ne l'est pas ou ce qui l'est moins ; |
| **7** | Planifier la prévention ; |
| **8** | Prendre les mesures de protection collective et leur donner la priorité sur les mesures de protection individuelle ; |
| **9** | Donner des instructions appropriées. |

### 8.1.3 Dispositif spécifique au SAIVAJ

- Textes de référence :

- fiche 1 B 9 du plan national de prévention et de lutte « Pandémie grippale » : suivi des indicateurs de situation ;
- circulaire du ministre de la fonction publique du 26 août 2009. Pandémie grippale : gestion des ressources humaines dans la fonction publique (NOR : BCFF0919655C) et ses 5 fiches annexes : (1) présence des agents (poursuite de l'activité sur le lieu du travail, autorisation d'absence, restriction des activités non essentielles, travail à distance, contribution à la continuité du service) ; (2) conditions d'exercice du droit de retrait ; (3) aménagement de l'organisation et du temps de travail ; (4) rémunération ; (5) rôle des chefs de service et des médecins de prévention.

#### 8.1.3.1 Indicateur d'absentéisme

- Principe :

L'indicateur d'absentéisme constitue l'élément de base de l'observation par le ministre coordinateur du SAIVAJ de la capacité des établissements à assurer la continuité des activités d'importance vitale qui leur incombent. Sur instruction du HFDS, l'indicateur est activé, sous l'autorité directe des chefs de cour de zone de défense et de sécurité, par les chefs de département ressources humaines et actions

sociales des plateformes interrégionales de service. Il n'est pas spécifique à la planification « pandémie grippale ».

La synthèse nationale de l'indicateur d'absentéisme constitue une des missions d'importance vitale incombant à l'opérateur d'importance SDAC (service de l'administration centrale) ; elle relève de la responsabilité du chef du bureau de l'action sociale et des conditions de travail (BASCT) qui anime le réseau d'action sociale du SAIVAJ.

Les plans de sécurité d'opérateur des OIV rattachés au SAIVAJ (DSJ, DAP, DPJJ, SDIT, Conseil d'État) tiennent à jour la liste des correspondants des chefs de département ressources humaines et actions sociales des plateformes interrégionales de service, chargés du recueil zonal des éléments de l'indicateur. Ils organisent également l'arborescence du réseau de recueil des données aboutissant au correspondant du chef de département.

Les indicateurs sont réunis, en fonction des instructions données, à un rythme hebdomadaire (la journée du mardi étant recommandée par les services), bihebdomadaire (mardi et jeudi) ou même journalier ; ils sont adressés parallèlement en copie, pour ce qui concerne les juridictions administratives, au directeur de l'accueil et de la sécurité du Conseil d'État.

- Modèle type d'indicateur d'absentéisme :

Un modèle type de recueil d'indicateur sur tableur est adressé par le BASCT aux chefs de département ressources humaines et actions sociales. Les plans de sécurité d'opérateur des OIV rattachés au SAIVAJ (DSJ, DAP, DPJJ, Conseil d'État) intègrent ce même modèle afin d'en organiser la généralisation à l'ensemble des services.
Le modèle zonal prend la forme suivante :

| **PLATEFORME INTERREGIONALE DE ……<br>INDICATEUR D'ABSENTEISME EN DATE DU 00/00/0000** | | | |
|---|---|---|---|
| **Nom de la personne en charge du dossier** | | - | |
| **Coordonnées téléphoniques** | | - | |
| **Adresse courriel** | | | |
| Départements | **Effectif d'agents affectés dans les services (1)** | **Nombre d'agents absents, toutes causes confondues (2)** | **% d'agents présents** |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **N° Dept** | | | |
| **Total** | | | |

**(1) Cette donnée est invariable.**
(2) dont les arrêts maladie ordinaires, les congés, les congés de longue maladie, *etc*.

- Organisation du réseau d'action sociale du SAIVAJ :

| ORGANISATION DU RESEAU D'ACTION SOCIALE DU SAIVAJ | | | | |
|---|---|---|---|---|
| **ZONE D'ACTION** | **SERVICE** | **FONCTION** | **Nom du titulaire** | **Téléphone** |
| **Ministère de la justice** | Bureau de l'action sociale et des conditions de travail | Chef du bureau | Stéphanie RENAUD | 01 70 22 71 66 |
| | | Médecin coordinateur national | Docteur Nadine TRAN QUY | 01 70 22 72 01 |
| | | Chef du pôle élaboration des politiques | Mathieu STOECKEL | 01 70 22 91 92 |
| | | Ingénieur-préventeur Coordinateur national | N… | |
| | | Conseiller national en travail social | N…… | |
| **Administration centrale** | département des ressources humaines de l'administration centrale | Chef du département | Marc Teissier | 01 44 77 75 25 |
| | | Médecin de prévention | Docteur Thibaut CROCHET | 01 70 22 70 10 |
| | | Conseiller régional en travail social | Marie-Laure POMMIER | 06 08 61 11 58 |
| | | Secrétariat | | 01 44 77 72 54 |
| **ZDS NORD** | Plateforme interrégionale de LILLE Départements 02 – 59 – 60 – 62 - 80 | Chef du département ressources humaines et action sociale | Anne-Laure HEROGUEL | 03 22 97 58 93 |
| | | Médecin coordinateur régional | Docteur Richard DYMNY | 06 61 37 21 67 |
| | | Conseiller régional en travail social | Anne-Marie LEULLIER | 06 79 86 58 98 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Olivier CASALS | 03 62 23 81 56 |
| | | Secrétariat | | 03 22 97 58 94 |
| **ZDS PARIS** | Plateforme interrégionale de PARIS Départements (PFI coordonnatrice) 75 – 77 – 78 - 91 – 92 – 93 – 94 - 95 | Chef du département ressources humaines et action sociale | Dominique SINGER | 01 53 62 20 83 |
| | | Médecin coordinateur régional | Docteur Raymond BESSARD | 06 70 61 14 59 |
| | | Conseiller régional en travail social | Marie-Laure POMMIER | 06 08 72 60 98 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | N…. | 01 44 32 71 19 |
| | | Secrétariat | | 01 44 32 72 89 |
| | Plateforme interrégionale de DIJON Département 89 | Chef du département ressources humaines et action sociale | Jean-Yves RASETTI | 03 45 21 51 38 |
| | | Médecin coordinateur régional | Docteur Jacqueline TAILLARDAT | 06 07 53 84 36 |
| | | Conseiller régional en travail social | N……. | 07 77 69 52 09 |
| | | Secrétariat | | 03 45 21 51 44 |
| **ZDS OUEST** | Plateforme interrégionale de RENNES (PFI coordonnatrice) Départements 14 – 22 – 29 – 35 – 44 – 49 – 50 – 53 – 56 – 61 - 72 | Chef du département ressources humaines et action sociale | Marie-Christine GENDRY | 02 90 09 32 24 |
| | | Médecin coordinateur régional | Docteur Bruno DULIERE | 06 70 61 17 26 |
| | | Conseiller régional en travail social | Franck CHAUSSADE | 06 19 22 31 36 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | N…. | 02 90 09 32 29<br>06 19 22 31 36 |
| | | Secrétariat | | 02 90 09 32 26 |
| | Plateforme interrégionale de PARIS Départements 18 – 28 – 37 – 41 – 45 - 36 | Chef du département ressources humaines et action sociale | Dominique SINGER | 01 53 62 20 83 |
| | | Médecin coordinateur régional | Docteur Raymond BESSARD | 06 70 61 14 59 |
| | | Conseiller régional en travail social | Marie-Laure POMMIER | 06 08 72 60 98 |

| | | | | |
|---|---|---|---|---|
| | Plateforme interrégionale de LILLE<br>Départements<br>27 - 76 | Référent hygiène – sécurité – conditions de travail - handicap | N…. | 01 44 32 71 19 |
| | | Secrétariat | | 01 44 32 72 89 |
| | | Chef du département ressources humaines et action sociale | Anne-Laure HEROGUEL | 03 22 97 58 93 |
| | | Médecin coordinateur régional | Docteur Richard DYMNY | 06 61 37 21 67 |
| | | Conseiller régional en travail social | Anne-Marie LEULLIER | 06 79 86 58 98 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Olivier CASALS | 03 62 23 81 56 |
| | | Secrétariat | | 03 22 97 58 94 |
| **ZDS SUD-OUEST** | Plateforme interrégionale de BORDEAUX<br>(PFI coordonnatrice)<br>Départements<br>16 – 17 – 19 – 23 – 24 – 33 – 40 – 64 – 79 - 86 - 87 | Chef du département ressources humaines et action sociale | Frédérique BEURRIER-DESCUDET | 05 56 79 76 43 |
| | | Médecin coordinateur régional | Docteur Françoise CONSTANTIN | 06 07 53 85 90 |
| | | Conseiller régional en travail social | Benoît PELLOQUIN | 06 32 64 81 13 |
| | | Chef du département ressources humaines et action sociale | Carine BOURIAT | 05 35 38 92 45 |
| | | Secrétariat | | 05 56 79 76 46 |
| | Plateforme interrégionale de TOULOUSE<br>Départements<br>47 – 09 – 31 – 32 – 46 – 65 – 81 - 82 | Chef du département ressources humaines et action sociale | Isabelle AMARI | 05 62 20 61 36 |
| | | Médecin coordinateur régional | Docteur Patrick MARCHANDOT | 06 17 01 22 84 |
| | | Conseiller régional en travail social | Josette DEBORDE | 06 18 45 03 18 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Jean-Marc LANTOURNE | 05 62 20 61 04<br>06 31 95 87 62 |
| | | Secrétariat | | 05 62 20 61 29 |
| | Plateforme interrégionale de RENNES<br>Département<br>85 | Chef du département ressources humaines et action sociale | Marie-Christine GENDRY | 02 90 09 32 24 |
| | | Médecin coordinateur régional | N….. | 06 70 61 17 26 |
| | | Conseiller régional en travail social | Franck CHAUSSADE | 06 19 22 31 36 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | N….. | 02 90 09 32 29<br>06 19 22 31 36 |
| | | Secrétariat | | 02 90 09 32 26 |
| **ZDS SUD** | Plateforme interrégionale de AIX-EN-PROVENCE<br>(PFI coordonnatrice)<br>Départements<br>04 – 06 – 13 – 83 -2A – 2B | Chef du département ressources humaines et action sociale | Brigitte CAMAU | 04 42 91 51 41 |
| | | Médecin coordinateur régional | N…… | 06 77 33 78 06 |
| | | Conseiller régional en travail social | Marièle CONTE | 06 32 64 81 01 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Claire LAVESQUE | 04 42 91 51 47<br>06 72 07 70 93 |
| | | Secrétariat | | 04 42 91 51 45 |
| | Plateforme interrégionale de TOULOUSE<br>Départements<br>84 – 11 – 12 – 30 – 34 – 48 – 66 - 07 | Chef du département ressources humaines et action sociale | Isabelle AMARI | 05 62 20 61 36 |
| | | Médecin coordinateur régional | Docteur Patrick MARCHANDOT | 06 17 01 22 84 |
| | | Conseiller régional en travail social | Josette DEBORDE | 06 18 45 03 18 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Jean-Marc LANTOURNE | 05 62 20 61 04<br>06 31 95 87 62 |

| | | | | |
|---|---|---|---|---|
| | | Secrétariat | | 05 62 20 61 29 |
| **ZDS SUD-EST** | Plateforme interrégionale de LYON (PFI coordonnatrice) Départements 01 – 03 – 05 - 15 – 26 – 38 – 42 – 43 – 63 – 69 – 73 - 74 | Chef du département ressources humaines et action sociale | Jean-Christophe SENEZ | 04 72 84 60 97 |
| | | Médecin coordinateur régional | N….. | 06 77 33 54 88 |
| | | Conseiller régional en travail social | Maryse LABIT | 06 46 33 57 96 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Blandine PUTHET | 04 27 01 24 36 |
| | | Secrétariat | | 04 73 64 62 01 |
| **ZDS EST** | Plateforme interrégionale de NANCY (PFI coordonnatrice) Départements 47 – 67 – 68 – 88 – 54 - 55 | Chef du département ressources humaines et action sociale | Daniel RAVENEY | 03 88 23 90 50 |
| | | Médecin coordinateur régional | Docteur Philippe MASSON | 06 08 61 80 06 |
| | | Conseiller régional en travail social | Béatrice YAGER | 06 72 62 73 92 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Laura BLANC GONNET | 03 54 95 31 57 |
| | | Secrétariat | | 03 88 23 90 51 |
| | Plateforme interrégionale de DIJON Départements 08 – 10 – 21 – 51 – 52 – 71 – 25 – 39 – 70 – 90 - 58 | Chef du département ressources humaines et action sociale | Jean-Yves RASETTI | 03 80 74 95 49 |
| | | Médecin coordinateur régional | Docteur Jacqueline TAILLARDAT | 06 07 53 84 36 |
| | | Conseiller régional en travail social | N…… | 06 32 64 81 63 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Vanessa RIVA | 03 45 21 51 45 |
| | | Secrétariat | | 03 80 74 95 48 |
| **OUTRE-MER** | Plateforme interrégionale de TOULOUSE | Chef du département ressources humaines et action sociale | Isabelle AMARI | 05 62 20 61 36 |
| | | Médecin coordinateur régional | Docteur Patrick MARCHANDOT | 06 17 01 22 84 |
| | | Conseiller régional en travail social | Josette DEBORDE | 06 18 45 03 18 |
| | | Référent hygiène – sécurité – conditions de travail - handicap | Jean-Marc LANTOURNE | 05 62 20 61 04<br>06 31 95 87 62 |
| | | Secrétariat | | 05 62 20 61 29 |

### 8.1.3.2 Rôle des médecins de prévention

Sous l'autorité des chefs de cour d'appel de zone de défense et de sécurité, les chefs de département ressources humaines et actions sociales des plateformes interrégionales prennent les contacts utiles avec l'ensemble des chefs des services déconcentrés du ministère de la justice ainsi qu'avec les présidents des juridictions administratives pour organiser en liaison avec les médecins coordonnateurs l'information des personnels, notamment pour ce qui concerne les mesures collectives et individuelles d'hygiène à mettre en œuvre, ainsi que les modalités de collecte des éléments nécessaires au renseignement des indicateurs destinés à l'information des chefs de cour de zone de défense et du BASCT.

Dans le même cadre, les médecins coordonnateurs régionaux organisent les interventions des médecins de prévention au bénéfice des services et des juridictions administratives. Les médecins de prévention assurent un rôle de conseil de l'administration et des organisations professionnelles et à ce titre doivent :

– aider l'administration à procéder à une évaluation des risques afin que celle-ci soit en mesure de mettre en place des dispositifs de prévention collective adéquats ;
– informer sur les règles spécifiques de prévention du risque biologique ;
– rappeler à l'administration et aux agents les règles d'hygiène de base (lavage des mains, *etc*.), l'intérêt du port des équipements de protection individuelle, *etc*. ;
– intervenir, en cas d'infection supposée, pour informer et prendre les mesures de prévention nécessaires. Le chef de service doit veiller à ce que la personne contaminée ou suspectée de l'être ne soit en contact avec le reste du personnel jusqu'à son départ du service ;
– conseiller à la personne contaminée de consulter, sans délai, un médecin de ville ;
– informer parallèlement le médecin coordonnateur régional et l'antenne régionale d'action sociale (ARAS) concernés ;
– prêter une attention particulière à l'état des équipements sanitaires, à leur entretien, ainsi qu'à la régularité de l'approvisionnement en produits d'hygiène.

#### 8.1.3.3 Principales règles d'hygiène face à un risque épidémique

Les principes d'hygiène à observer sont efficaces contre les maladies infectieuses à transmission respiratoire et de nombreuses autres pathologies (gastro-entérites, *etc*.) et doivent être mis en œuvre de façon permanente dans les services :

- Discipline comportementale individuelle :

– cn cas de toux ou d'éternuement, se couvrir la bouche et le nez afin de ne pas augmenter la transmission par voie aérienne, notamment par les gouttelettes respiratoires ;
– se moucher avec des mouchoirs en papier à usage unique jetés dans une poubelle pourvue d'un sac plastique ; ne cracher que dans un mouchoir en papier à usage unique, jeté dans une poubelle pourvue d'un sac plastique.

- Hygiène des mains :

– le lavage des mains au savon – ou même avec des produits hydro-alcooliques (vendus en parapharmacie) – est essentiel. Il doit être fait soigneusement et répété très souvent dans la journée, et d'autant plus par les personnes travaillant dans un cadre collectif ;
– la disponibilité des produits d'hygiène doit faire l'objet d'un suivi attentif des autorités hiérarchiques.

- Nettoyage fréquent :

– dans les locaux de travail, nettoyage des surfaces de contact (poignées de porte, chasses d'eau, meubles, *etc*.) à l'eau chaude et au savon ou avec des produits désinfectants.

- Gestion appropriée des déchets :

– les poubelles doivent être pourvues de sacs plastique munis d'un lien de fermeture et changés fréquemment.

#### 4.1.1.1 Port de moyens de protection respiratoire

- Texte de référence :

– haut Conseil de la santé publique, avis du 1er juillet 2011 relatif à la stratégie à adopter concernant le stock État de masques respiratoires.

| INDICATIONS<br><br>concernant le port de différents moyens de protection respiratoire en population générale en cas d'émergence d'un agent respiratoire hautement pathogène<br><br>**L'hygiène des mains est une mesure systématiquement associée.** | | | |
|---|---|---|---|
| **Groupe de la population** | **Type de masque** | **Durée du port** | **Commentaire** |
| Cas suspects, possibles ou confirmés | Masque anti-projection | Période de contagiosité | Nécessité de disposer de masques pédiatriques de différentes tailles.<br>Mise à disposition de masques, d'information, de solutés hydro-alcooliques dans tous les lieux de soins |
| Personnes vivant dans l'entourage immédiat d'un cas suspect, possible ou confirmé et contribuant à ses soins | Masque anti-projection | Période de contagiosité du sujet malade, lors d'un contact : fréquentation d'un même espace clos (pièce, véhicule) | |
| Personnes se rendant dans des lieux publics ou se déplaçant en transport en commun | Masque anti-projection | Lors de la fréquentation de ces lieux | |

| Indications professionnelles concernant le port de différents moyens de protection respiratoire en cas d'émergence d'un agent respiratoire hautement pathogène | | | |
|---|---|---|---|
| Personnels exposés au risque du fait de leur profession (exemple : métiers de guichet) ; ne concerne pas les professions de santé et filières animales « à risque » | Masque anti-projection | Pendant la durée d'exposition | |
| Personnels directement exposés à un risque élevé : personnels de santé exposés, personnels de laboratoire, personnels de secours, personnels des établissements de ramassage et de traitement des déchets, personnels des filières animales concernées en cas d'agent à transmission zoonotique (particulièrement avicoles et porcines) | APR de type FFP2 (ou capacité filtrante supérieure) | Pendant la durée d'exposition | Selon la situation, port d'équipements complémentaires (gants, lunettes, vêtements de protection, combinaison, bottes) |

# 9 Annexe PROCÉDURES D'EXPLOITATION DE LA SÉCURITÉ

Les procédures d'exploitation de la sécurité s'appliquent aux services reliés au réseau privé virtuel de la justice.

## *9.1 Gestion des comptes à privilège*

### 9.1.1 Objet

La procédure d'exploitation de la sécurité (PES) s'applique pour l'ensemble des comptes à privilège des systèmes d'information du ministère de la justice et sans exception aux opérateurs agissant sur les SI pour le compte du ministère de la justice qu'ils soient des agents du ministère ou des prestataires externes.

- Son application et son contrôle interne sont de la responsabilité de la chaîne fonctionnelle SSI du ministère.
- Elle définit pour les comptes à privilège :

– la gestion des comptes systèmes natifs ;
– la nomenclature des comptes systèmes opérationnels ;
– la stratégie des mots de passe ;
– la procédure de création de compte ;
– la procédure de suppression de compte ;
– la gestion des absences prolongées ;
– l'imputabilité ;
– les procédures de contrôle et la documentation adéquate.

### 9.1.2 Domaine d'application

- Sont définis comme comptes à privilège, les comptes permettant des actions de gestion, de paramétrage, d'accès à des ressources systèmes.
- Sont considérées comme ressources systèmes prioritaires :

– les serveurs en « *data center* » et les serveurs locaux ;
– les systèmes de gestion de base de données ;
– les équipements et les systèmes d'infrastructure (SAN, NAS, SI de sauvegarde, AD, LDAP) ;
– les équipements actifs de réseau (EAR) ;
– les équipements et les systèmes de sécurité (FW, SIEM, IGC) ;
– les postes de travail.

- Remarque : les comptes d'administration fonctionnelle des applications métier ne sont pas inclus dans le champ de cette procédure.

### 9.1.3 Gestion des comptes à privilège

#### 9.1.3.1 Comptes d'administration natifs

- L'accès et l'usage des comptes d'administration natifs sont interdits. En effet, le partage de ces identités entre techniciens ne permet pas une traçabilité et une imputabilité conformes aux exigences de sécurité imposées par les avis de la CNIL et du Conseil d'État dans le cadre des applications métier.
    - Il convient dans l'ordre de priorité suivante, et, en fonction des possibilités techniques d'appliquer les mesures suivantes :

– désactiver techniquement ces comptes ;
– empêcher l'utilisation par la mise en place d'un mot de passe inconnu des techniciens ;
– limiter strictement à un accès local après authentification nominative préalable en dernier recours.

    - Le dossier d'exploitation du serveur devra indiquer et justifier le mode de protection.

#### 9.1.3.2 Constitution des identifiants des comptes d'administration opérationnels

    - L'authentification doit permettre une identification non équivoque. L'accès à toute ressource est accordé par une identification nominative. Pour les comptes à privilège, un préfixe composé de trois lettres est ajouté.
    - Les deux premières lettres correspondent au périmètre de compétence technique :

– sy : pour les administrateurs systèmes ;
– bd : pour les administrateurs de base de données ;
– rx : pour les administrateurs réseaux ;
– pt : pour les administrateurs des postes de travail ;
– se : pour les CSSI effectuant des tâches d'administration de la sécurité ;
– di : pour les administrateurs systèmes et réseau, uniquement en DIT ;
– cl : pour les correspondants locaux informatique des directions métier ;

    - La troisième lettre correspond au type de ressource humaine :

– i : pour les personnes internes au ministère de la justice ;
– e : pour les personnes externes (partenaires et prestataires) ;

    - Remarque : Pour les correspondants locaux, le trigramme sera toujours « cli. » ;

Exemples :
– un agent du MJ administrateur système : syi.prénom.nom ;
– un prestataire administrateur de base de données : bde.prénom.nom ;
– un prestataire intervenant sur les postes de travail : pte.prénom.nom ;
– un agent du MJ administrateur système et réseau en DIT : dii.prénom.nom ;

#### 9.1.3.3 Mécanismes d'authentification

    - Les mécanismes d'authentification suivants sont mis en œuvre :

– authentification par composant cryptographique avec des certificats électroniques fournis par l'infrastructure de gestion de clefs SDIT ;
– authentification par mot de passe respectant un niveau de complexité élevé.

- Remarque : pour les « *data center* », l'accès aux serveurs par mot de passe ne peut s'effectuer qu'après une authentification forte sur le système « Accès administrateur ».

- Stratégie des mots de passe :

Par défaut la stratégie minimale suivante des mots de passe est mise en œuvre :
– antériorité maximale du mot de passe : 90 jours ;
– antériorité minimale du mot de passe : 1 jour ;
– historique des mots de passe : 10 mots de passe ;
– exigence de complexité : activé (minuscules/majuscules/caractères spéciaux/numériques) ;
– longueur minimale du mot de passe : 12 caractères.

#### 9.1.3.4 Procédure de création de compte

- La procédure de création de compte respecte les obligations suivantes :

– demande du responsable hiérarchique/fonctionnel incluant la date de fin de mission pour les personnes externes ;
– vérification de conformité par le correspondant SSI (fonction, droits, préfixe de l'identifiant) ;
– validation par : à déterminer ;
– création du compte ;
– remise de l'authentifiant, rappel des obligations et signature de l'attestation de responsabilité par le correspondant SSI ;
– contrôle mensuel en liaison avec les autorités hiérarchiques par le correspondant SSI.

#### 9.1.3.5 Procédure de suppression de compte

- La procédure de suppression de compte respecte les obligations suivantes :

– départ signalé par le responsable hiérarchique ou fonctionnel ;
– désactivation immédiate du compte ;
– validation par le chef de département ;
– contrôle mensuel par le CSSI ;
– suppression après 36 mois (voir gestion des traces) ;
– détailler par département : Annexe n° 2 - Suppression d'un compte à privilège au sein du département « XXX ».

#### 9.1.3.6 Gestion des absences prolongées

– lors d'absence supérieure à deux semaines, les comptes sont désactivés ;
– le responsable hiérarchique ou fonctionnel doit informer le gestionnaire de compte avant la période d'absence pour désactivation et au retour de l'utilisateur pour réactivation ;
– détailler par département : Annexe n°3 - Gestion des absences prolongées des « externes » au sein du département « XXX ».

#### 9.1.3.7 Inactivité des comptes

- Les comptes inutilisés depuis plus trois semaines sont désactivés à la demande du CSSI. Les comptes de secours, qui peuvent déroger à cette règle, doivent être répertoriés et des mesures de contrôle spécifiques doivent être mises en œuvre pour s'assurer qu'ils ne sont pas utilisés à d'autres fins.

- Ils sont réactivés à la demande :

– de l’utilisateur pour les utilisateurs internes ;
– du responsable hiérarchique pour les externes.

- Détailler par département : Annexe n°4 - Inactivité des comptes au sein du département « XXX ».

#### 9.1.3.8 Imputabilité

– toutes les actions réalisées avec des comptes à privilège sont journalisées et conservées pendant 36 mois ;
– cette journalisation respecte les mesures de sécurité définies dans la déclaration d’applicabilité (DdA).

#### 9.1.3.9 Procédures de contrôle

- CSSI : les correspondants SSI sont responsables de la sécurité opérationnelle au sein de leur département. À ce titre, ils doivent :

– veiller à une utilisation légitime et justifiée des comptes d’administration natifs ;
– s’assurer des modalités de restriction d’usage mises en place sur les comptes d’administration natifs ;
– contrôler que les personnes agissant sur le SI disposent des privilèges adéquats ;
– effectuer une revue des comptes et des privilèges au minimum 1 fois tous les 3 mois ;
– rendre compte au RSSI de toute utilisation anormale.

- RSSI SDIT : après validation par le comité SSI, le RSSI peut demander un audit des comptes à privilège en s’appuyant sur une équipe technique composée de CSSI. À l’issue, le RSSI SDIT doit :

– informer le chef de département des résultats de l’audit ;
– élaborer avec le responsable de département et le CSSI le plan d’amélioration.

## *9.2 Gestion des outils et des données en mobilité*

### 9.2.1 Objet

Il s’agit de définir la procédure d’exploitation de la sécurité (PES) pour l’ensemble des moyens liés à la mobilité intégrés aux systèmes d’information du ministère de la justice.

### 9.2.2 Domaine d’application de la PES

- Elle s’applique sans exception à l’ensemble des personnels du ministère de la justice qu’ils soient des agents du ministère ou des prestataires externes.
- Elle définit les politiques concernant :

– les supports de mémoires amovibles (CD, DVD, USB, SD, Micro SD, *etc*.) ;
– les outils de traitement de l’information (ordiphones, tablettes, ordinateurs portables, *etc*.) ;
– les données du ministère en cas de mobilité.

### 9.2.3 Gestion des supports de mémoires amovibles

– est entendu comme support de mémoire amovible, tout support physique permettant le stockage d’informations numériques, nativement indépendant du ou des matériels pouvant lire et exploiter

les informations qu'il conserve (disquettes, CD, DVD, disques durs externes, USB, carte SD, carte micro SD, *etc*.) ;
– de manière générale les supports de mémoires amovibles n'ont pas vocation à assurer l'archivage ou la sauvegarde des documents du fait du manque de fiabilité de ces supports dans le temps et du risque de divulgation massive d'informations en cas de perte.

#### 9.2.3.1 Supports de mémoires amovibles autorisés

– les seuls supports de mémoires amovibles autorisés à s'interconnecter avec les SI du ministère sont ceux fournis par le ministère ;
– la seule exception recevable est celle des clefs des partenaires/prestataires du ministère de la justice dans le cadre d'échanges volumineux.

#### 9.2.3.2 Condition d'usage des supports de mémoires amovibles

– tout support de mémoire amovible doit, préalablement à sa lecture, faire l'objet d'un scan anti-virus ;
– à l'exception des administrateurs, l'exécution de scripts ou de fichiers binaires depuis un support de mémoire amovible est prohibé ;
– un support de mémoire amovible fourni par le ministère est considéré comme un élément du SI du ministère et ne peut donc être interconnecté que sur les SI du ministère. La seule exception recevable est liée aux échanges de fichiers volumineux avec les partenaires/prestataires du ministère de la justice ;
– les informations stockées sur les supports de mémoire amovibles doivent l'être conformément aux règles édictées par la PMDS (6.1.1), ce qui doit se concrétiser par le chiffrement des données stockées dès que la sensibilité de ces dernières ne permet pas de les considérer comme publiques.

### 9.2.4 Gestion des outils de traitement de l'information

De manière générale, il convient de retenir que l'usage ou l'interconnexion de moyens autres que ceux mis à disposition par le ministère sur les SI du ministère sont prohibés. La réalisation des missions assurées par le ministère doit se faire avec les outils confiés par le ministère.

#### 9.2.4.1 Ordinateurs portables

- Les ordinateurs portables utilisés par les personnels du ministère qu'ils soient des agents du ministère ou des prestataires externes doivent être fournis, gérés et administrés par les services informatiques et télécommunications du ministère.
- Ces ordinateurs doivent nécessairement respecter les préconisations de l'étude de sécurité du poste de travail réalisée par la SDIT, ce qui implique que de manière non exhaustive :

– l'accès au paramétrage matériel (*setup*) doit être verrouillé par un mot de passe et la séquence de démarrage (*boot*) doit être restreinte au disque dur local ;
– les paramètres de connexion ne peuvent pas être modifiés par l'utilisateur et les mots de passe sont conformes à la PMDS ;
– les utilisateurs ne sont pas administrateurs de leur poste ;
– les mises à jour doivent être automatisées ;
– un anti-virus est présent, à jour, et l'analyse temps réel est activée ;
– l'installation de logiciels sur le poste ou de composants supplémentaires dans le navigateur et le client de messagerie ne doit pas être techniquement possible ;

– le droit d'exécution doit être retiré sur les répertoires et les fichiers utilisateur ou temporaire ;
– les paramètres de sécurité JAVA sont restreints et non modifiables par l'utilisateur ;
– le pare-feu local doit être actif en entrée et en sortie ;
– seuls les flux identifiés, documentés et autorisés au niveau national sont ouverts en entrée ;
– l'accès à Internet doit être réalisé via des relais (*proxy*) effectuant une analyse de contenu ;
– le service de partage doit être désactivé, les partages administratifs doivent être désactivés et aucun service de type serveur ne doit être activé sur un poste client.

- Pour ce qui concerne les ordinateurs portables, il conviendra d'appliquer les règles suivantes :

– lors d'une connexion filaire au RPVJ, toutes les autres interfaces réseau doivent être désactivées (*Wi-Fi*, 3G, *etc*.) ;
– la configuration réseau interdit toute connexion à internet en dehors de la solution de *VPN* mise en œuvre par le ministère ;
– le mot de passe du client *VPN* ne peut être mémorisé dans l'application ;
– le disque dur est chiffré au niveau système.

#### 9.2.4.2 Tablettes

– les tablettes doivent être considérées comme des ordinateurs portables. La mise en œuvre et l'utilisation de ces dernières doit respecter les procédures et règles applicables aux ordinateurs portables (dans la limite des moyens techniques existants) ;
– si une puce GPS est incluse, les fonctions de géolocalisation doivent être désactivées sur les applications autres que celles liées à la cartographie ;
– si une carte SIM est intégrée il convient d'appliquer les règles relatives à la « gestion des terminaux mobiles » (voir 9.2.4.3).

#### 9.2.4.3 Téléphones mobiles et ordiphones

– les téléphones mobiles et ordiphones doivent être considérés comme des tablettes. La mise en œuvre et l'utilisation de ces derniers doit respecter les procédures et règles applicables aux tablettes dans la limite des moyens techniques existants ;
– il convient, en l'absence de raccordement filaire au RPVJ, de s'assurer que le téléphone ou l'ordiphone mis en œuvre est géré de façon centralisée à l'aide d'un outil de « gestion de terminaux mobiles » (voir 9.2.4.3).

#### 9.2.4.4 Systèmes divers

- Lecteurs multimédia :

– la connexion des lecteurs multimédia, sauf s'ils sont la propriété du ministère, est interdite sur les systèmes d'information du ministère et ce, même pour les recharger, l'interconnexion de ce type de support étant un vecteur privilégié pour les virus et autres codes malveillants ;
– il est a fortiori prohibé de faire installer un logiciel d'interface avec cette typologie de produit sur les SI du ministère (exemple : le branchement d'un lecteur mp3 sur le port USB de l'ordinateur de bureau est interdit).

- GPS :

– la connexion des GPS pour mise à jour, sauf s'ils sont la propriété du ministère, est interdite sur les systèmes d'information du ministère, même pour les recharger ;
– il est a fortiori prohibé de faire installer un logiciel d'interface avec cette typologie de produit sur les SI du ministère.

### 9.2.5 Gestion des données du ministère en mobilité

- Hébergements et transferts des données sensibles du ministère :

– conformément à la PMDS et sauf accord explicite du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation, les données sensibles du ministère ne doivent être hébergées que sur le territoire national ;
– seuls les systèmes d'information du ministère répondent aux exigences réglementaires. L'usage de systèmes de stockage en ligne - tels que DropBox, skyDrive, Google drive, ou d'échanges, tels que WeTransfer, SendBox, TransferNow, *etc*. qui ne satisfont notamment pas à ce prérequis, est prohibé.

## *9.3 Cryptographie & protocoles de communication sécurisés*

### 9.3.1 Objet

Les mécanismes cryptographiques et protocoles les utilisant doivent suivre les recommandations suivantes.

### 9.3.2 Domaine d'application

Tous.

### 9.3.3 Documents de référence

- Définitions et terminologies spécifiques :

– AES : Advanced Encryption Standard ;
– ECDHE : Elliptic Curve Diffie-Hellman ;
– ECDSA : Elliptic Curve Digital Signature Algorithm ;
– DES : Data Encryption Standard ;
– DHE : Diffie-Hellman key Exchange ;
– DSS : Digital Signature Standard ;
– HMAC : keyed-Hash Message Authentication Code ;
– IANA : Internet Assigned Numbers Authority ;
– RSA : Rivest Shamir Adleman ;
– TLS : Transport Layer Security ;
– SSL : Secure Socket Layer ;
– SSH : Secure Shell.

### 9.3.4 Contexte général

La cryptographie moderne a mis à disposition des architectes des systèmes d'information, une série d'outils permettant de garantir un certains nombres de fonctions de sécurité. Dans la littérature, ces outils sont appelés algorithmes cryptographiques ou mécanismes cryptographiques.

- Il existe deux grandes familles d'algorithmes de cryptographie :

– les algorithmes symétriques : ils utilisent une même clé appelée clé secrète pour toutes les opérations ;
– les algorithmes asymétriques : ils utilisent une paire de clés pour effectuer leurs opérations. Une clé sera alors qualifiée de clé privée qui, par définition ne devra en aucun cas être communiquée, tandis qu'une autre clé sera alors qualifiée de clé publique.

- Les fonctions de sécurité que peuvent garantir ces algorithmes sont résumées dans le tableau ci-dessous :

| ***Service*** | | ***Cryptographie symétrique*** | ***Cryptographie asymétrique*** |
|---|---|---|---|
| Confidentialité | | Chiffrement par bloc ou par flot | Chiffrement à clé publique |
| Intégrité | | Code d'authentification du message | Echange de clés |
| Authentification | de données | | Signature numérique |
| | d'entités | Défi-réponse | |
| Non-répudiation | | n.a | |

- Il est à noter que dans les protocoles actuels de communication sécurisés (TLS, SSH, *etc*.), les deux types d'algorithmes sont utilisés pour l'établissement d'un canal sécurisé et il est nécessaire de recourir à des algorithmes et des tailles de clé adéquats pour garantir une robustesse optimale.
- Face à la diversité des outils disponibles, la politique d'exploitation et de sécurité donne le cadre de d'utilisation et de paramétrage des algorithmes et des protocoles de communication afin de garantir un état de l'art cohérent vis-à-vis des recommandations en vigueur en cryptographie.

### 9.3.5 Recommandations sur les algorithmes cryptographiques

#### 9.3.5.1 Algorithmes symétriques

Dans la famille des algorithmes symétriques, il existe deux types de primitives de chiffrement pour garantir la confidentialité : le chiffrement par bloc et le chiffrement par flot. Les règles ci-après ne concernent que les algorithmes de chiffrement par bloc qui sont les plus utilisés et représentatifs au sein des implémentations techniques.

- Algorithmes et tailles de clés :

– les algorithmes choisis et les tailles de clé doivent être compatibles avec les exigences du RGS ;
– la liste des algorithmes et des tailles de clés recommandées se trouvent au 9.3.8.

- Utilisation / Gestion :

– une clé secrète doit être associée à un seul usage ;
– la génération de la clé secrète doit être effectuée sur le système qui héberge l'applicatif utilisant la clé secrète ;
– la clé secrète ne doit pas quitter le système sur lequel elle est stockée ;
– *a minima*, les droits d'accès à la clé secrète doivent être restreints en lecture/écriture (Permissions POSIX -r-------- ou 600) au seul service devant y accéder.

#### 9.3.5.2 Algorithmes asymétriques

- Algorithmes et tailles de clés :

– les algorithmes choisis et les tailles de clés doivent être compatibles avec les exigences du RGS ;
– la liste des algorithmes et des tailles de clés recommandées se trouvent en 9.3.8.

- Utilisation/ Gestion :

– une bi-clé doit être associée à un seul usage ;
– la génération des bi-clés doit être effectuée sur le système qui héberge l'applicatif utilisant la clé privée ;
– la partie de la bi-clé appelée clé privée ne doit pas quitter le système sur lequel elle est stockée ;
– les droits d'accès à la partie de la bi-clé appelé clé privée doivent être restreints en lecture/écriture (Permissions POSIX -r-------- ou 600) au seul service devant y accéder.

### 9.3.6 Algorithmes de hachage

Les algorithmes de hachage ou fonctions de hachage sont très souvent employés de concert avec les algorithmes cryptographiques afin de garantir, dans l'enchaînement des actions nécessaires pour établir une communication chiffrée, certaines fonctions de sécurité. Il convient d'établir des recommandations destinées à utiliser correctement les bons algorithmes.

- Algorithmes et tailles de condensat :

– les algorithmes choisis et les tailles de clés doivent être compatibles avec les exigences du RGS ;
– la liste des algorithmes et des tailles de condensat recommandés se trouvent en 9.3.8.

### 9.3.7 Protocoles de communications sécurisés

#### 9.3.7.1 Secure Socket Layer / Transport Layer Security (SSL/TLS)

- SSL/TLS est un protocole ayant pour fonction de créer un canal de communication authentifié, protégé en confidentialité et en intégrité. TLS est l'évolution normalisée de SSL par l'IETF. Le but initial de ce protocole était de sécuriser le protocole HTTP mais les applications se sont considérablement étendues aux autres protocoles de communication n'offrant pas nativement autant de fonctions de sécurité telles que LDAP, POP, IMAP, SMTP.

- Depuis la création de SSL/TLS l'utilisation des versions sécurisées de ces protocoles s'est largement répandue et un certain nombre de vulnérabilités ont été découvertes. La sécurité globale des échanges ne dépend donc plus uniquement de l'implémentation de SSL/TLS mais également de son paramétrage.

– La version minimale du protocole à utiliser lors d'une connexion SSL/TLS DOIT être TLS 1.0.

- Lors de la négociation TLS, le client envoie un message CLIENT HELLO qui contient une liste de ciphers supportés. Le serveur choisit parmi cette liste la combinaison qu'il préfère pour établir la communication. De ce fait, configurer une liste de suites cryptographiques (ou ciphersuite) dans un ordre précis permet de contrôler les ciphers qui sont utilisés entre le client et le serveur.

- Une ciphersuite se compose comme suit :

– algorithme d'échange de clés ;
– authentification de l'échange de clés ;
– chiffrement des flux de données ;
– hachage.

Exemple en notation IANA : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

– la gestion des suites cryptographiques doit respecter la liste des suites cryptographiques présentes en 9.3.8 (attention cette ciphersuite est affichée en notation OpenSSL). Pour implémenter cette

ciphersuite dans une configuration Apache, il convient de la copier dans la directive de configuration SSLCipherSuite ;
– les certificats électroniques doivent être issus de l'autorité de certification appelée « AC Technique ».

#### 9.3.7.2 Secure Shell (SSH)

- SSH est un protocole de communication permettant d'ouvrir un shell sur un serveur distant. Le mode de fonctionnement de SSH requiert des clés de chiffrement pour garantir la confidentialité et l'intégrité des messages transitant sur un canal non-sûr. SSH fut créé pour remplacer Telnet et les autres protocoles de communication non-sûrs comme rsh. Le serveur le plus utilisé est OpenSSH qui a été développé par les créateurs d'OpenBSD. Dans le cadre de la PES, les directives de configuration citées seront celles d'un serveur OpenSSH.

– la version du protocole SSH utilisée doit être la version 2 (directive Protocol 2) ;
– la gestion des suites cryptographiques doit respecter la liste des suites cryptographiques présentes en 9.3.8 ; pour implémenter cette ciphersuite dans une configuration OpenSSH, il convient de la copier dans la directive de configuration Ciphers.

#### 9.3.7.3 IPSec

- Le protocole IPSec a été défini par l'IETF pour combler les manques du protocole IP en matière de sécurité. Ainsi, les communications établies avec ce protocole sont authentifiées et chiffrées. IPSec peut être utilisé pour protéger un flux de données entre deux hôtes, deux passerelles de sécurité ou entre un hôte et une passerelle de sécurité. Un tunnel IPSec est constitué d'une paire de Security Association ou SA unidirectionnel qui spécifie les données de contexte du protocole telles que : IP source/IP destination, le mode (tunnel ou transport) et les protocoles employés (AH ou ESP), les algorithmes cryptographiques employés, les clés associées à cet algorithme.

– le protocole IPSec doit utiliser le protocole ESP pour garantir la confidentialité et l'intégrité des échanges ;
– le protocole IPSec doit être mis en œuvre en mode tunnel pour garantir la confidentialité des entêtes IP internes ;
– le protocole IKE en version 2 doit être utilisé pour la négociation dynamique des algorithmes et clés d'une SA.

- Le protocole IKE est constitué de deux phases :

<u>La phase de création du canal sécurisé ou phase 1 :</u>
– le mode secret partagé ou pre-shared key ne doit pas être utilisé ;
– le mode agressif (« agressive mode ») ne devrait pas être utilisé ;
– des certificats électroniques doivent être utilisés.

<u>La phase négociation des SA ou phase 2 :</u>
– le mode secret partagé ou pre-shared key ne doit pas être utilisé ;
– le renouvellement périodique des clés devrait être paramétré à 1 heure ;
– le groupe Diffie-Hellman ne doit pas être le groupe 1 ou le groupe 2.

- Les algorithmes et tailles de clés paramétrés doivent être ceux définis en 9.3.8.

### 9.3.8 Annexes

#### 9.3.8.1 Liste des protocoles autorisés par type

- Algorithmes symétriques compatibles avec le RGS :

– les algorithmes suivants doivent être utilisés : 3DES, RC5, AES, RC6, Camelia, Serpent.

- Algorithmes asymétriques compatibles avec le RGS :

– les algorithmes suivants doivent être utilisés : RSA (chiffrement), DSA (Signature), ElGamal (Signature).

- Fonction de hachage :

– les algorithmes suivants ne doivent pas être utilisés : MD5, SHA-1 ;
– les algorithmes suivants doivent être utilisés : SHA256, SHA512, BLAKE, Skein.

#### 9.3.8.2 Recommandations sur la taille des clés et condensats

- Algorithmes symétriques :

– la taille d'une clé secrète doit être au minimum de 128 bits.

- Algorithmes asymétriques :

– la taille du module doit être au minimum de 2048 bits.

- Fonction de hachage :

– la taille du condensat doit être au minimum de 256 bits.

#### 9.3.8.3 Liste des suites cryptographiques (ou cipher-suite)

- Ciphersuite OpenSSL

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:AES128:AES256:RC4-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!3DES:!MD5:!PSK

- Ciphersuite OpenSSH

aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,
chacha20-poly1305@openssh.com

## *9.4 Mise au rebut des matériels*

### 9.4.1 Objet

Procédure d'exploitation de la sécurité définissant les règles de mise au rebut des matériels et équipements informatiques.

### 9.4.2 Domaine d'application

Tout matériel contenant des informations traitées par les systèmes d'information du ministère si celui-ci contient un support de stockage de masse : disque dur, fax, imprimante (multifonctions), en réseau ou non, acheté ou loué.

### 9.4.3 Documents de référence

- instruction interministérielle 901/SGDSN/ANSSI du 28/01/2015 relative à la protection des systèmes d'information sensibles ;
- guide technique 972-1/SGDSN/DCSSI du 17/07/2003 pour la confidentialité des informations enregistrées sur les disques durs à recycler ou à exporter ;
- article du CERT-IST du 01/08/2006 sur l'effacement sécurisé de disques durs ;
- IGI n° 1300.

### 9.4.4 Définitions et terminologie spécifiques

- support réutilisable : média qui permet l'écriture de telle façon que les données précédemment écrites peuvent devenir inaccessibles dans les conditions normales d'exploitation du média ;
- support magnétique : média sur lequel des données sont écrites et lues grâce à des champs magnétiques ; un support magnétique est réutilisable par nature ;
- disque dur : système constitué d'un ou plusieurs supports magnétiques, appelés plateaux, et d'un sous-système, appelé têtes, composé d'éléments mécaniques, électroniques et logiques, qui effectue les transcriptions, l'écriture et la lecture des données ;
- écriture : opération qui place des signaux magnétiques rémanents sur les plateaux ;
- lecture : opération qui mesure les signaux magnétiques rémanents sur les plateaux ;
- effacement : opération qui supprime les signaux magnétiques rémanents sur les plateaux ;
- accès logique : méthode d'acquisition de données au moyen des têtes du disque dur contrôlées soit par la logique implantée dans ces têtes, soit par une autre logique ;
- accès physique : méthode d'acquisition de données avec des moyens d'investigation sensibles aux traces perceptibles directement sur les plateaux ;
- recyclage : changement dans l'emploi d'un disque dur sans changer d'environnement de sécurité ;
- exportation : envoi d'un disque dur hors de son environnement de sécurité.

### 9.4.5 Contexte général

- Les équipements en réseau du ministère ne contiennent pas d'informations classifiées.
- Les niveaux de confidentialité définis par la DNS sont :

- 0 – Faible ou nul (C0) ;
- 1 – Diffusion limitée (C1) ;
- 2 – Diffusion restreinte (C2) ;
- 3 – Secret (C3).

### 9.4.6 Gestion de la cession d'équipements

- R-01 : Obligation de procéder ou de faire procéder à la destruction des supports et des équipements informatiques par des personnes habilitées et qualifiées pour ces opérations ;
- R-02 : Obligation de procéder à un contrôle (ex : identification, marquage, enregistrement de sortie) de tous les équipements (exemple : ordinateurs portables, postes de travail) envoyés en

réparation, recyclés pour un nouvel usage (ex : changement de service), cédés à des tiers ou mis au rebut ;
- R-03 : Interdiction de céder les matériels avec les éventuelles licences logicielles qui s'y trouveraient (ex : OS, suite bureautique, *etc*.) qui doivent rester la propriété du ministère ;
- Obligation de gestion de la mise au rebut des équipements.

#### 9.4.6.1 Stockage des biens destinés à la mise au rebut

- R-04 : Obligation de stocker les documents sensibles et les biens désignés en attente de destruction dans une zone de travail, sur le site ou à l'extérieur, dans des conteneurs adaptés ou dans des zones de sécurité.

#### 9.4.6.2 Préparation de la mise au rebut

- R-05 : Obligation dans le cas de la mise au rebut d'un poste ***Utilisateur***, de vérifier avec l'agent à qui a été attribué le poste de travail que les données ont été sauvegardées (si nécessaire) ;
- R-06 : Obligation, pour un ***Serveur***, de vérifier avec l'administrateur en charge de son exploitation que les données ont été sauvegardées (si nécessaire).

#### 9.4.6.3 Règles de mise au rebut

*Mise au rebut des équipements*
- R-07 : Obligation de contrôler avant de sortir de l'établissement tous les équipements (ex : ordinateurs portables, postes de travail) envoyés en réparation, recyclés pour un nouvel usage (ex : changement de service), cédés à des tiers ou mis au rebut (ex : identification, marquage, enregistrement de sortie) ;
- R-08 : Obligation d'effacer toutes les données présentes sur les supports (ex : disque dur) en utilisant un procédé adapté (exemple : procédure de suppression et de surcharge des supports de données) ;
- R-09 : Obligation de démonter et détruire les équipements pour lesquels les opérations de suppression ne pourraient être réalisées (ex : panne du support de stockage).

*Mise au rebut des disques et supports amovibles*
- R-10 : Obligation d'effacer de manière à les rendre irrécupérables les données stockées sur les disques durs (exemple : interne, extractible, externe) ou les supports amovibles (exemple : disques durs externes, CD, DVD, clés USB, disquettes, bandes magnétiques) suivant un procédé adapté (exemple : procédure de suppression et de surcharge des supports de données) lorsqu'ils sont mis au rebut.

#### 9.4.6.4 Protocole de mise au rebut

- R-11 : Obligation de procéder à un effacement du ou des supports avec un dispositif d'effacement renforcé tel que (dans l'ordre de préférence) :
  1 - Solution matérielle (démagnétiseur/degausser) ;
  2 - Solution logicielle qualifiée/certifiée par l'ANSSI (ex : solutions logicielles BLANCCO : Fiche ANSSI de certification CC et EAL3+ de la version 5 : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cc/certificat_2012_04.html ; Fiche ANSSI de qualification standard de la version 4.8 : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/p_31_Blancco_Data_Cleaner+_version_4.8.html ; Site de BLANCCO : http://www.blancco.com/fr/accueil/ ) ;
  3 - Solution logicielle validée par le ministère (ex : solution logicielle DBAN (Site de DBAN : http://sourceforge.net/projects/dban/) ou ddblank présent dans la distribution SCALPEL) ;
  4 - Formatage du disque dur de bas niveau avec un minimum de 3 passes ;

- R-12 : La sous-direction de l'informatique et des télécommunications du ministère de la justice a déployé dans tous les DIT des démagnétiseurs qualifiés pour ses besoins propres de mise au rebut, ces équipements étant mis à la disposition des autres services du ministère. Il est obligatoire de recourir à ces équipements pour procéder à la mise au rebut de biens avant d'avoir recours aux solutions dégradées ;
- R-13 : En cas d'impossibilité de procéder à un effacement respectant l'une des procédures de la règle ***R-12***, par exemple si le support de stockage ne peut pas subir de surcharge de sécurité (CD-R, disque dur défectueux *etc.*), le service gestionnaire doit lui-même, ou par le biais d'une société spécialisée, procéder à sa destruction physique (séparation en plusieurs éléments du support initial) ;
- R-14 : Dans tous les cas, un procès-verbal de destruction doit être rédigé et validé par l'autorité hiérarchique du service gestionnaire ;
- R-15 : Comme pour les matériels obsolètes, le matériel détruit doit ensuite être pris en charge par une société spécialisée dans le traitement de ces déchets.

#### *9.4.6.4.1 Cas particulier des supports de stockage d'éléments de chiffrement et cryptographiques*

- R-16-1 : Dans le cas particulier des supports de stockage d'éléments servant à gérer ou mettre en œuvre des solutions de chiffrement et/ou à gérer ou mettre en œuvre des solutions cryptographiques, ces support doivent être détruits physiquement selon les règles en vigueur , même si ces solutions ou l'usage qui en est fait ne relèvent pas de la protection du secret de la défense nationale (ex : outil de mise en œuvre d'une PKI, disques durs ayant servi de stockage à des clés privées, *etc*.).

### 9.4.6.5 Prise en compte de la mise au rebut dans les contrats

- R-16-2 : Obligation de prévoir explicitement dans les contrats de maintenance ou de location, qu'en cas de retrait du matériel, les supports de stockage (disques durs) seront enlevés et remplacés par des supports effacés (surcharge de sécurité) par le ministère.

### 9.4.6.6 Sensibilisation des utilisateurs

R-16-3 : Dans le cas d'informations sensibles, l'utilisateur doit être sensibilisé aux obligations suivantes :

- détruire les documents papier (ex : utilisation de broyeur / déchiqueteur) et prendre les mesures de protection appropriées pendant leur destruction ;
- détruire les supports magnétiques sensibles (ex : disque dur, CD-ROM, clé USB) au moyen de réécriture ou de démagnétisation afin que les informations soient effacées de manière sûre.

### 9.4.6.7 Moyens de contrôle

- Gestion des événements, journalisation :

- R-17 : Obligation de conserver à des fins d'audit la liste des supports et des équipements recyclés pour un nouvel usage (exemple : changement de service), cédés à des tiers, détruits ou mis au rebut. La durée de conservation de cette liste est fixée à ? ans ;
- R-18 : Obligation d'enregistrer toute destruction en mentionnant au minimum le lieu, la date, l'heure, le type de matériel, sa référence et la personne et/ou l'entité ayant procédé à la destruction ;
- R-19 : Obligation de mettre à disposition des RCSSI de la SDIT et des directions ayant le besoin d'en connaître tous les registres de destruction des matériels en cas de demande de ces derniers.

#### *9.4.6.7.1 Audit*

– R-20 : Obligation de procéder à un contrôle des registres de destructions au minimum une fois par an, cet audit devant être piloté par le RCSSI, qui pourra déléguer cette mission aux RISSI ;
– R-21 : Obligation de procéder à un contrôle par échantillonnage des matériels mis au rebut afin de vérifier la bonne exécution de la procédure, ces contrôles devant être effectués au minimum une fois par trimestre, l'audit devant être piloté par le RCSSI, qui pourra déléguer cette mission aux RISSI.

# 10 SIGLES ET ACRONYMES

| | |
|---|---|
| AGRASC | : agence de gestion et de recouvrement des avoirs saisis et confisqués |
| ALDS | : agent local de défense et de sécurité |
| ANSSI | : agence nationale de sécurité des systèmes d'information |
| APJ | : agent de police judiciaire |
| APIJ | : agence publique pour l'immobilier de la justice |
| ARS | : agence régionale de santé |
| BASCT | : bureau de l'action sociale et des conditions de travail |
| BYOD | : *bring your own device* (utilisation d'équipements informatiques personnels) |
| CA | : cour d'appel |
| CAA | : cour administrative d'appel |
| CAZDS | : cour d'appel de zone de défense et de sécurité |
| CCAZDS | : chefs de cour d'appel de zone de défense et de sécurité |
| CDCS | : centre de crise et de soutien (MAE) |
| CEF | : centre éducatif fermé |
| CHS | : comité d'hygiène et de sécurité |
| CHSCT | : comité d'hygiène, de sécurité et des conditions de travail |
| CIC | : cellule interministérielle de crise |
| CIAV | : cellule interministérielle d'aide aux victimes |
| CNDA | : cour nationale du droit d'asile |
| CNDSAJ | : comité national de défense et de sécurité des activités judiciaires |
| CNIL | : commission nationale de l'informatique et des libertés |
| CPDS | : comité de pilotage de la défense et de la sécurité |
| CCPM | : cellule de crise du Premier ministre |
| CD | : centre de détention |
| CE | : Conseil d'État |
| CE | : chef d'établissement |
| CIAV | : cellule interministérielle d'aide aux victimes |
| CNDSAJ | : comité national de défense et de sécurité des activités judiciaires |
| COG | : commandant des opérations de gendarmerie |
| COP | : commandant des opérations de police |
| CORRUSS | : centre opérationnel de réception et de régulation des urgences sanitaires et sociales |
| COS | : commandant des opérations de secours |
| CPDS | : comité de pilotage de la défense et de la sécurité |

CTP : comité technique paritaire

CSL : centre de semi-liberté

CSL : correspondant sûreté local

CSR : correspondant sûreté régional

CMZ : chargé de mission zonal

CUMP : cellule d'urgence medico-psychologique

CZDSAJ : comité zonal de défense et de sécurité des activités judiciaires

DACG : direction des affaires criminelles et des grâces

DACS : direction des affaires civiles et du sceau

DAP : direction de l'administration pénitentiaire

DCDS : délégué central à la défense et à la sécurité

DDS : délégué à la défense et à la sécurité

DECT : *digital enhanced cordless telephone* (standard de communication téléphonique sans fil)

DIA-DISP : directeur interrégional adjoint des services pénitentiaires

DIDS : délégué interrégional à la défense et à la sécurité

DILGA : délégation interministérielle à la lutte contre la grippe aviaire

DIPJJ : direction intérrégionale de la protection judiciaire de la jeunesse

DISP : direction interrégionale des services pénitentiaires

DNSAJ : directive nationale de sécurité des activités judiciaires

DOS : direction des opérations de secours

DPJJ : direction de la protection judiciaire de la jeunesse

DSJ : direction des services judiciaires

DSP : directeur des services pénitentiaires

DZDS : délégué zonal à la défense et à la sécurité

EBIOS : expression des besoins et identification des objectifs de sécurité

ENAP : ecole nationale d'administration pénitentiaire

ENG : école nationale des greffes

ENM : ecole nationale de la magistrature

EOPELFI : établissement public d'exploitation du livre foncier informatisé

EPE : établissement de placement éducatif

EPEI : établissement de placement éducatif et d'insertion

EPM : établissement pour mineurs

EPRUS : établissement de préparation et de réponse aux urgences sanitaires

EPSNF : établissement public de santé de Fresnes

ESIR : expert sûreté interrégional

FAO : food and agriculture organization (Organisation des nations unies pour l'agriculture et l'alimentation)

FENVAC : fédération nationale des victimes d'attentats et d'accidents collectifs

FGTI : fonds de garantie des victimes d'actes de terrorisme et autres infractions

FSSI : fonctionnaire de sécurité des systèmes d'information

HFDS : haut-fonctionnaire de défense et de sécurité

IGI : instruction générale interministérielle

IGSJ : inspection générale des services judiciaires

IHEDN : Institut des hautes études de la défense nationale

INAVEM : institut national d'aide aux victimes et de médiation

INTERPOL : organisation internationale de police criminelle (OIPC)

IPBX : PABX utilisant le protocole Internet IP pour véhiculer les communications

IVC : identification des victimes de catastrophes

JIRS : juridiction interrégionale spécialisée

MA : maison d'arrêt

MC : maison centrale

MERS : Middle East respiratory syndrome (coronavirus)

NIR : numéro d'inscription au répertoire des personnes physiques

OIE : Office international des épizooties, devenu Organisation mondiale de la santé animale

OIS : officier interrégional de sécurité

OIV : opérateur d'importance vitale

OMS : Organisation mondiale de la santé

OPJ : officier de police judiciaire

ORSEC : organisation de la réponse de sécurité civile

PABX : *private automatic branch exchange* (autocommutateur téléphonique privé)

PCA : plan de continuité d'activité

PDA : personnal digital assistant (ordiphone)

PES : procédure d'exploitation de la sécurité

PFI : plateforme interrégionale

PG : procureur général

PIV : point d'importance vitale

PMDS : politique ministérielle de défense et de sécurité

PP : premier président

PP : plan de protection

PPP : plan particulier de protection
PPE : plan de protection externe
PPSMJ : personne placée sous main de justice
PR : procureur de la République
PSO : plan de sécurité opérateur
PUMP : poste d'urgence medico-psychologique
QCD : quartier centre de détention
QMA : quartier maison d'arrêt
QMC : quartier maison centrale
QPA : quartier pour peines aménagées
RCS : référentiel complémentaire de sécurité
RSSI : responsable de sécurité des systèmes d'information (appelation générique)
RCSSI : responsable central de sécurité des systèmes d'information
RGI : responsable de gestion informatique
RIE : réseau interministériel de l'Etat
RISSI : responsable interrégional de la sécurité des systèmes d'information
RLSSI : responsable local de la sécurité des systèmes d'information
RNDS : référentiel national de défense et de sécurité
RPVJ : réseau privé virtuel du ministère de la justice
RSO : référentiel de sécurité opérateur (PSO + RCS)
RZSSI : responsable zonal de la sécurité des systèemes d'information
SADJAV : service de l'accès au droit et à la justice et de l'aide aux victimes
SAIV : secteur d'activités d'importance vitale
SAIVAJ : secteur d'activités d'importance vitale des activités judiciaires
SAMU : service d'aide médicale urgente
SAR : service administratif régional
SDAC : service de l'administration centrale
SDIT : sous-direction de l'informatique et des télécommunications
SEAT : service éducatif auprès du tribunal
SECJD : service éducatif du centre pour jeunes détenus de Fleury-Mérogis
SEEPM : service éducatif au sein d'établissement pénitentiaire pour mineurs
SG : secrétariat général du ministère de la justice
SGCA : secrétaire général de cour d'appel
SGCAZDS : secrétaire général de cour d'appel de zone de défense et de sécurité
SGDSN : secrétariat général de la défense et de la sécurité nationale

SI : système(s) d'information

SINUS : système d'information numérique standardisé

SMS : *short message system* (messagerie élémentaire sur téléphones mobiles)

SPIP : service pénitentiaire d'insertion et de probation

SRAS : syndrome respiratoire aigu sévère

STEI : service territorial éducatif et d'insertion

STEMO : service territorial éducatif de milieu ouvert

STEMOI : service territorial éducatif de milieu ouvert et d'insertion

SSI : sécurité des systèmes d'information

TA : tribunal administratif

TI : tribunal d'instance

TGI : tribunal de grande instance

UE : Union européenne

UEAJ : unité éducative d'activités de jour

UEAT : unité éducative auprès du tribunal

UESEAT : unité rattachée au service éducatif auprès du tribunal

UESEEPM : unité des services éducatifs au sein d'un établissement pénitentiaire pour mineurs

UECER : unité éducative centre éducatif renforcé

UEHD : unité éducative d'hébergement diversifié

UEHC : unité éducative d'hébergement collectif

UEMO : unité éducative de milieu ouvert

UIVC : unité d'identification des victimes de catastrophes

USB : universal serial bus (standard de connexion de périphériques informatiques)

ZDS : zone de défense et de sécurité