Cadre commun de la sécurité des systèmes d'information et de télécommunications

Sommaire

1. Introduction . . . . . page 09

1.1 Contexte et enjeux . . . . . page 09
1.2 Objet . . . . . page 10
1.3 Révision du Cadre du Cadre Commun de la Sécurité des Systèmes d'Information . . . . . page 14
1.4 Champ d'application . . . . . page 14
1.5 Définitions . . . . . page 15

2. Principes de sécurité liés au personnel . . . . . page 16

2.1. Sensibilisation . . . . . page 16
Article 1. Principes généraux . . . . . page 16
Article 2. Rôle des Personnes Juridiquement Responsables (PJR) . . . . . page 16
Article 3. Rôle des Responsables de la Sécurité des Systèmes d'Information . . . . . page 16
Article 4. Rôle de l'encadrement . . . . . page 17

2.2. Responsabilités . . . . . page 17
Article 1. Principes généraux . . . . . page 17
Article 2. Management de la sécurité . . . . . page 17
Article 3. Principe de séparation des responsabilités . . . . . page 18
Article 4. La responsabilité des Personnes Juridiquement Responsables (PJR) . . . . . page 18
Article 5. La responsabilité des RSSI . . . . . page 18
Article 6. La responsabilité des Correspondants de Sécurité . . . page 19
Article 7. La responsabilité des utilisateurs . . . . . page 19

3. Principes de sécurité liés à l'information . . . . . page 19

3.1 Protection des informations . . . . . page 19

3.2 Typologie des informations ou ressources nécessitant une protection . . . . . page 20
Article 1. Principes généraux . . . . . page 20
Article 2. Les critères d'évaluation de la sensibilité . . . . . page 20
Article 3. Le niveau de sensibilité . . . . . page 21
Article 4. Le niveau de confidentialité . . . . . page 21
Article 5. Typologies des menaces . . . . . page 22
Article 6. Gravité du risque . . . . . page 22
Article 7. Croisement de la sensibilité des biens, des menaces et de la gravité des risque . . . . . page 23

3.3 Protection des informations . . . . . page 24
Article 1. Principes généraux . . . . . page 24
Article 2. La gestion de document classifié . . . . . page 24
Article 3. Protection des informations stockées ou traitées . . . . page 25

4. Principes de sécurité liés aux systèmes informatiques et de télécommunications . . . . . page 26

4.1 Protection des systèmes informatiques et de télécommunications . . . . . page 26
Article 1. Principes généraux . . . . . page 26
Article 2. Responsabilités . . . . . page 27

4.2 Gestion des systèmes informatiques et de télécommunications . . . . . page 27
Article 1. Principes généraux . . . . . page 27
Article 2. Définition des zones de confiance du ministère . . . . . page 28
Article 3. Principe d'architecture sécurisée . . . . . page 31
Alinéa a. Principes Généraux . . . . . page 31
Alinéa b. Principe de réduction du risque . . . . . page 31
Alinéa c. Principe de proportionnalité . . . . . page 32
Alinéa d. Principe de subsidiarité . . . . . page 32
Alinéa e. Isolement des zones de confiance vis-à-vis de l'extérieur . . . . . page 32
Alinéa f. Zones de communication avec l'extérieur . . . page 33
Alinéa g. Accès au réseau Internet initialisés depuis une zone de confiance . . . . . page 33

5. Principes liés à l'organisation de la sécurité . . . . . page 33

5.1 Structure de la sécurité . . . . . page 33
Article 1. Principes généraux . . . . . page 33
Article 2. La Personne Juridiquement Responsable (PJR) . . . . . page 34
Article 3. Le Responsable de la Sécurité des Systèmes d'Information (RSSI) . . . . . page 34
Article 4. Les Correspondants de Sécurité . . . . . page 36

5.2 Continuité de contrôle de la sécurité . . . . . page 36

6. Principes de sécurité liés au cycle de vie du système d'information . . . . . page 37

6.1 Spécification pour le développement du système d'information . page 37
Article 1. Principes généraux . . . . . page 37
Article 2. Pilotage de la sécurité dans le cycle de vie des projets . page 40
Article 3. Création d'un espace de confiance pour la protection de l'information dans les projets . . . . . page 41
Article 4. Sécurité des développements informatiques et de la maintenance applicative . . . . . page 41
Article 5. Cadre méthodologique «Sécurité et Développement» . . page 42
Article 6. Les environnements d'exploitation . . . . . page 43
Article 7. Prestations de services externes . . . . . page 44

6.2 Autorisation pour l'utilisation du système d'information . . . . . page 44
Article 1. Principes généraux . . . . . page 44
Article 2. Principes de gestion des habilitations . . . . . page 45
Article 3. Sécurité logique et contrôle d'accès aux applications et informations . . . . . page 45
Alinéa a. Attribution et gestion des droits . . . . . page 45
Alinéa b. Processus d'identification et d'authentification page 46
Article 4. Règles s'appliquant aux administrateurs de systèmes informatiques . . . . . page 47

6.3 Exploitation sécurisée du système d'information . . . . . page 47
Article 1. Principes généraux . . . . . page 47
Article 2. Convention de service . . . . . page 48
Article 3. Exploitation des réseaux . . . . . page 49
Alinéa a. Principes . . . . . page 49
Alinéa b. Tenue d'une base d'informations sur les infrastructures réseaux, applicatives et cartographie . . page 49
Alinéa c. Configuration des équipements de réseau . . page 50
Alinéa d. Contrôle, détection et traitement des incidents réseaux et télécommunications . . . . . page 51
Article 4. Exploitation des systèmes . . . . . page 51
Alinéa a. Tenue d'une base d'informations . . . . . page 51
Alinéa b. Configuration des systèmes et des postes utilisateurs . . . . . page 52
Alinéa c. Règles de configurations . . . . . page 53
Alinéa d. Gestion des supports et média informatiques . page 53

6.4 Sécurité pour les échanges d'informations . . . . . page 53
Article 1. Principes généraux . . . . . page 53
Article 2. Les fichiers informatiques . . . . . page 54
Article 3. La messagerie électronique . . . . . page 54

6.5 (Télé)maintenance du système d'information . . . . . page 54
Article 1. Principes généraux . . . . . page 54
Article 2. Préparation et suivi de l'intervention . . . . . page 55

Article 3. Télé-maintenance . . . . . page 55
Article 4. Maintenance du matériel informatique . . . . . page 55
Article 5. Maintenance du matériel réseau et de télécommunications . . . . . page 56

6.6 Mise en place d'une documentation de sécurité . . . . . page 56
Article 1. Principes généraux . . . . . page 56
Article 2. Règles de gestion documentaire . . . . . page 56
Article 3. Règles relatives au Carnet de Sécurité des Systèmes d'Information . . . . . page 57

6.7 Limitation des sinistres du système d'information . . . . . page 58
Article 1. Principes généraux . . . . . page 58
Alinéa a. Plans de sauvegarde . . . . . page 58
Alinéa b. Plan de secours . . . . . page 59
Article 2. Tableaux de bords et Pilotage de la Sécurité . . . . . page 60

6.8 Application des ITSEC pour une évaluation de la sécurité du système d'information . . . . . page 62

6.9 Anticipation pour l'évolution de la sécurité du système d'information . . . . . page 62

1. Introduction

1.1 Contexte et enjeux

Chaque établissement comme chaque type d'application peut présenter des enjeux de sécurité qui lui sont spécifiques. Néanmoins, les risques inhérents des SI à la sécurité sont réels pour tous. Par ailleurs, les systèmes d'information croissent en complexité mais font également l'objet d'une plus grande ouverture vers l'extérieur avec ses conséquences en terme d'exposition aux risques.
Sachant qu'il n'existe ni sécurité absolue, ni solution passe-partout en matière de sécurisation du système d'information, il s'agira dans ce document de définir, les procédures ou principes conduisant à une mise en œuvre efficace de la sécurité.

En effet, le Cadre Commun de la Sécurité des Systèmes d'Information doit déterminer les principes permettant d'assurer le niveau de sécurité adapté à chaque site. Il devra donc :

- fixer les règles communes permettant la cohérence générale du niveau de sécurité du système d'information de l'Éducation nationale;
- définir une méthode pour prendre en compte des besoins de sécurité tout au long du cycle de vie des systèmes d'information : de la conception à la mise en production et la maintenance ;
- fournir un cadre d'interopérabilité des politiques de sécurité en maîtrisant les risques et enjeux à chacun des niveaux du système éducatif (de l'école à l'université en passant par les services administratifs) ;
- définir, sensibiliser puis former les communautés éducatives aux problématiques de la sécurité des Systèmes d'Information ;
- mettre à la disposition des maîtrises d'ouvrage ainsi que des maîtrises d'œuvre, un outil d'analyse et d'expression de besoins ;
- guider les décideurs dans la mise en œuvre des politiques de sécurité appliquées aux établissements ou services dont ils ont la responsabilité.

L'information et la communication au sein des communautés éducatives nécessitent d'intégrer des exigences nouvelles en matière

des systèmes d'information afin de garantir la disponibilité, l'intégrité, la confidentialité des sytèmes d'information ainsi que la traçabilité des accès.

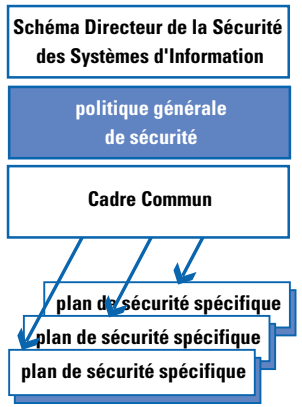
1. 2 Objet

Dans le cadre du Schéma Stratégique des Systèmes d'Information et de Télécommunications (S3IT), un comité de pilotage a été créé pour suivre et coordonner l'élaboration du Schéma Directeur de Sécurité des Systèmes d'information (SDS SI).
Le présent document dénommé «Cadre Commun de la Sécurité des Systèmes d'Information» se décline par référence au SDS SI pour en préciser les orientations générales et permettre ainsi l'élaboration des Plans de Sécurité des Systèmes d'Information (PS2I) opérationnels au sein des académies ou établissements d'enseignement supérieur tant sur les plans techniques, organisationnels qu'humains.

Pour appréhender la place du Cadre Commun dans la démarche globale de sécurité des Systèmes d'information mise en oeuvre par le ministère, il convient de rappeler les principes retenus pour traiter la Sécurité des Systèmes d'Information (SSI). Ces principes sont présentés ci-après.
La **Politique de Sécurité des Systèmes d'Information**, telle que la définit la DCSSI, est formalisée dans un ensemble de documents applicables, des directives, procédures, codes de conduite, standards de l'industrie, règles organisationnelles et techniques, le tout ayant pour objectif la protection du système d'information d'un organisme ou d'une institution.
Elle traduit **la reconnaissance officielle de l'importance accordée** par la direction générale d'un organisme à la sécurité de son système d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables.

Tenant compte de ces principes, le référentiel de la sécurité des systèmes d'information du MENESR s'articule autour des documents de référence représentés dans le diagramme ci-dessous.

Référentiel SSI

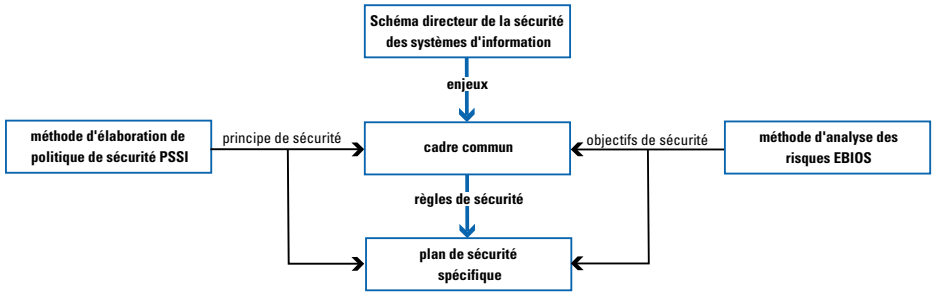


- Le Schéma Directeur de la Sécurité des Systèmes d'Information présente les **lignes directrices** de la Politique Générale de Sécurité. Ce schéma s'inscrit **à un niveau stratégique de sécurité**.
- Les Plans de Sécurité Spécifiques ou Types présentent les objectifs de sécurité nécessaires à la mise en application des règles du Cadre Commun de la Sécurité des Systèmes d'Information. Ils s'inscrivent au niveau opérationnel de sécurité.

Pour assurer la cohérence interne de ce référentiel de sécurité, le MENESR a adopté la démarche suivante :
- la stratégie de sécurité est définie au travers de lignes directrices, en amont, au plus haut niveau de la hiérarchie pour répondre directement aux enjeux du ministère ;
- les principes de sécurité qui en découlent sont identifiés au niveau fonctionnel par la mise en œuvre de méthodes recommandées au niveau interministériel par la DCSSI (cf. PSSI) ;
- en partant de ces **principes de sécurité**, les objectifs de sécurité spécifiques sont définis sur la base des risques réels identifiés au niveau opérationnel, en s'appuyant sur les résultats d'études d'évaluation des risques du type EBIOS, comme le recommande la DCSSI.

Ainsi, le cadre commun intègre tout à la fois **les enjeux du MENESR, les principes de sécurité retenus et les objectifs de sécurité définis.** Ce rôle pivot, permet de décliner, au travers de ce seul document, les règles de sécurité des plans de sécurité spécifiques, en cohérence des attentes du ministère et des contraintes du terrain.

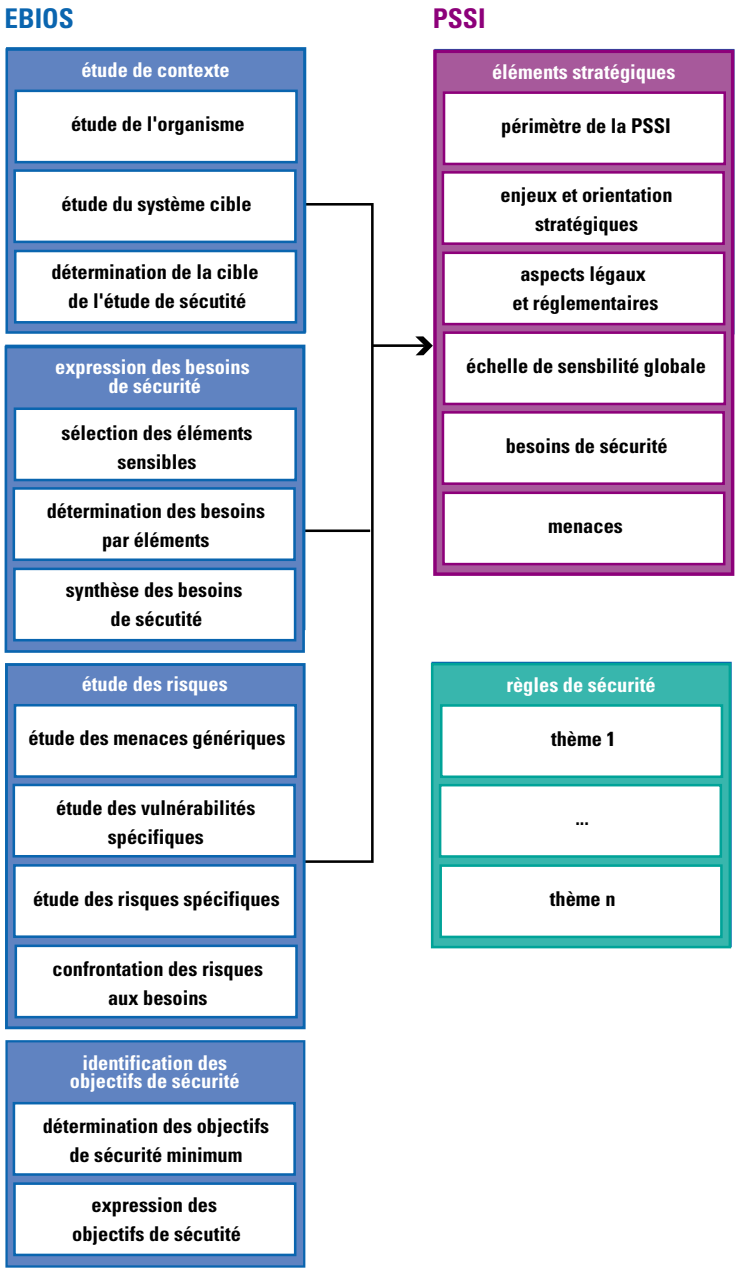
Cette démarche est illustrée dans la diagramme ci-dessous.



L'interopérabilité des démarches retenues devra favoriser la réutilisation des éléments étudiés. L'emploi de méthodes disposant d'un fort couplage telles que EBIOS et PSSI va dans ce sens. La réalisation préalable d'une étude EBIOS offre plusieurs avantages :

- l'élaboration de la politique SSI est facilitée par une démarche structurée qui permet d'obtenir l'ensemble des éléments stratégiques et d'élaborer les règles de sécurité ;
- les différents acteurs du SI (décideurs, responsables SSI, maîtrise d'oeuvre, maîtrise d'ouvrage, acteurs financiers, «utilisateurs»…) sont déjà sensibilisés à la SSI, notamment aux risques SSI et au fait que **la sécurité organisationnelle constitue une part essentielle de la sécurité globale.**

Les différentes étapes des démarches méthodologiques présentées ci-dessous peuvent être consultées depuis le site de la DCSSI (**http://www.ssi.gouv.fr**).



1.3 Révision du Cadre du Cadre Commun de la Sécurité des Systèmes d'Information

La politique générale ainsi que toute procédure de révision est à l'initiative d'une instance ad hoc composée notamment :

- d'un comité de pilotage ;
- du bureau des études techniques et des plans d'informatisation ;
- du réseau des RSSI ;
- du pôle de compétences SSI d'Aix-Marseille ;
- du Comité Réseau des Universités (CRU).

Ce document a pour vocation d'être mis à jour, a minima, bi-annuellement à compter de sa date de parution.
Des mises à jour pourront être envisagées suite à des évolutions des enjeux du MENESR relatifs à la SSI, entraînant des changements dans les orientations stratégiques de sécurité.
En outre, l'occurrence d'incidents de sécurité avérés sur le terrain, pourra essentiellement conduire à la révision du Cadre Commun de la Sécurité des Systèmes d'Information afin de permettre aux équipes en place de se doter des moyens nécessaires au traitement de ces incidents.

1.4 Champ d'application

Le Cadre Commun de la Sécurité des Systèmes d'Information s'applique à tous les personnels et établissements du ministère de l'Éducation nationale quelle que soit leur localisation géographique.
Le Cadre Commun de la Sécurité des Systèmes d'Information est décliné sous la forme de plans types afin de prendre en compte les besoins et les contraintes des établissements, des services administratifs centraux et déconcentrés.
Tous les établissements sous tutelle ou services du ministère doivent respecter et appliquer les dispositions de ce Cadre Commun de la Sécurité des Systèmes d'Information (CC SSI) mais également prendre en compte ses évolutions.

Le Cadre Commun de la Sécurité des Systèmes d'Information définit les mesures références de la SSI, mais, il ne dispense pas les responsables chargés de son application, de prendre des dispositions complémentaires en rapport avec leur contexte particulier.

1.5 Définitions

Aux fins de la présente politique, on entend par :
a) ministère : le ministère de l'Éducation nationale de l'Enseignement supérieur et de la Recherche ;
b) système d'information : l'ensemble des ressources fonctionnelles techniques et humaines qui permet de stocker, traiter, ou transmettre l'information ;
c) informations : l'ensemble des données et de leurs traitements à travers des applications ;
d) systèmes informatiques et de télécommunications : l'ensemble des ressources techniques, des supports de l'information, des moyens de communications et des supports de transmission des informations ;
e) sécurité informatique du système d'information : un concept qui recouvre un ensemble d'organisations, de méthodes, de techniques et d'outils mis en œuvre pour protéger les ressources d'un système d'information dans l'optique de satisfaire les besoins :

- de disponibilité : information, utilisable par une personne ou un système à la demande ;
- de confidentialité : information connue que des personnes ayant besoin de la connaître ;
- d'intégrité : information ne pouvant être ni altérée, ni détruite ou ni perdue par accident ou malveillance.

Pour satisfaire les besoins de disponibilité, d'intégrité, de confidentialité, la traçabilité ou l'auditabilité (la preuve) doit faire partie intégrante de la sécurité informatique.
C'est pourquoi, pour satisfaire les besoins pré-cités, les informations sont qualifiées en terme de vitales, stratégiques, sensibles ou personnelles ou ordinaires.

De même que les systèmes informatiques seront placés dans des zones qualifiées de vitales, stratégiques, sensibles ou non protégées.

2. Principes de sécurité liés au personnel

2.1 Sensibilisation

Article 1. Principes généraux

- La sensibilisation de tous les acteurs de la Sécurité des Systèmes d'Information doit être au cœur du dispositif de sécurité à mettre en place.
- La sensibilisation à la sécurité doit être adaptée aux différentes catégories de personnes.
- Toute personne doit savoir que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes d'information et de télécommunications.

Article 2. Rôle des Personnes Juridiquement Responsables (PJR)

Les Personnes Juridiquement Responsables doivent être particulièrement sensibilisées sur la responsabilité juridique qui leur incombe en matière de sécurité du système d'information. Elles jouent un rôle moteur dans la mise en place de l'organisation dédiée à l'application des mesures de sécurité définies dans le SDS SI et précisées dans par le présent document.

Article 3. Rôle des Responsables de la Sécurité des Systèmes d'Information

Les RSSI sont chargés d'animer et de contrôler la sécurité des systèmes d'information. Dans le cadre de cette mission, ils sont amenés notamment à organiser des sessions de formation à destination des responsables opérationnels sur leur rôle et devoir dans le domaine de la sécurité.

Article 4. Rôle de l'encadrement

La sensibilisation des personnes repose d'une part, sur le rôle des Personnes Juridiquement Responsables (PJR) qui impulsent politiquement les actions que les RSSI, avec l'appui de l'encadrement, mettent en œuvre dans le respect du cadre commun de la sécurité et d'autre part, sur les campagnes de sensibilisation régulières, menées sur le terrain.

2.2 Responsabilités

Article 1. Principes généraux

- La Personne Juridiquement Responsable (PJR) doit s'assurer que toutes les personnes de son établissement ont bien été sensibilisées à la sécurité du système d'information et qu'une chaîne opérationnelle de responsabilités est en place.
- La PJR doit, en fonction des contraintes de son établissement, évaluer les conditions d'accès aux informations et être en accord avec le niveau de sécurité défini par celles-ci.
- La délégation de compétence en matière de SSI dans une entité doit être clairement notifiée et acceptée par le responsable dépositaire dès sa prise de fonction.
- Toute personne est tenue de relayer les alertes au travers de la chaîne de responsabilités, et dans les plus brefs délais, de tout incident de sécurité sur les systèmes d'information.

Article 2. Management de la sécurité

Le management de la sécurité des systèmes d'information repose sur trois fondements :

- le RSSI est chargé de l'animation et du contrôle de la sécurité des systèmes d'information. Pour mener à bien cette mission, il s'appuie sur un adjoint et les correspondants de sécurité ;
- la responsabilisation directe des acteurs opérationnels dont la

fonction principale n'est pas d'assurer la sécurité mais d'intervenir dans les processus de mise en œuvre ;
- la sensibilisation des Personnes Juridiquement responsables (PJR) chargées de l'organisation des mesures de sécurité définies dans le Cadre Commun de la Sécurité des Systèmes d'Information.

Article 3. Principe de séparation des responsabilités

La politique de sécurité doit être animée par des personnes différentes de celles qui l'appliquent.
La séparation des responsabilités est essentielle pour l'application du Cadre Commun de la Sécurité des Systèmes d'Information. En effet, une personne ne doit pas se trouver à la fois en position de donneur d'ordre, de réalisateur et de contrôleur de bon achèvement.
Les rôles des certificateurs, développeurs et exploitants ne doivent pas être assumés par les mêmes individus.

Article 4. La responsabilité des personnes juridiquement responsables (PJR)

Ces personnes sont responsables de la mise en place d'une organisation chargée de mettre en oeuvre les mesures de sécurité définies dans le cadre commun de sécurité. À ce titre, la responsabilité des PJR est engagée dans le cas où une altération involontaire ou délibérée d'informations causerait un préjudice à une personne physique ou morale.

Article 5. La responsabilité des RSSI

Le RSSI est responsable de l'animation et du contrôle de la sécurité des systèmes d'information en fonction des objectifs de sécurité fixés par la PJR et dans le respect du Cadre Commun de la Sécurité des Systèmes d'Information. Il fait régulièrement état de la sécurité et relaie les alertes notamment en cas de risque majeur. Membre du réseau national des RSSI, il relaie au niveau local l'ensemble des préconisations et expertises mutualisées au niveau national.

Les RSSI peuvent être responsables de plusieurs sites en mettant en place les délégations nécessaires.

Article 6. La responsabilité des Correspondants de Sécurité

Les Correspondants de Sécurité sont chargés de la **mise en œuvre de la sécurité** au sein d'une entité donnée.
Les Correspondants de Sécurité mettent en oeuvre les règles générales d'exploitation, consignées dans le carnet de sécurité des systèmes d'information, règles pouvant être complétées par des mesures liées aux spécificités de l'entité.

Article 7. La responsabilité des «utilisateurs»

Les droits et devoirs des «utilisateurs» sont définis par une charte en fonction des catégories d'usagers : personnels, «administrateurs», élèves. Tout «utilisateur» ou usager constatant un incident, doit en rendre compte à son correspondant de sécurité ou à défaut, à son responsable hiérarchique qui déclenche une procédure de remontée d'alertes.

3. Principes de sécurité liés à l'information

3.1 Protection des informations

Voir aussi **chapitre 3 - 3.3 - (Article 2.** La gestion de document classifié)

Toute personne a un devoir de protection des informations qu'elle utilise ou qui lui sont confiées afin de diminuer le risque de détournement ou d'appropriation par des tierces personnes.
Le Guide Juridique de «l'utilisateur» associé à la charte des personnels de l'Éducation nationale, expose les règles légales qui s'imposent à tout personnel public, notamment en ce qui concerne l'obligation de neutralité (religieuse, politique et commerciale), de réserve, de discrétion et de respect des secrets protégés par la loi.

3.2 Typologie des informations ou ressources nécessitant une protection

Article 1. Principes généraux

- Toute information fera l'objet d'une classification explicite.
- La sensibilité d'une information ou d'une ressource est évaluée en fonction de l'impact qu'aurait sur l'organisation en cas de divulgation, dégradation, modification ou d'indisponibilité de celle-ci ou d'une ressource quelconque.
- Plusieurs critères de sécurité permettent de classer afin de déterminer les mesures de sécurité à adopter en regard des risques encourus.
- Le coût de la sécurité dépend du coût du risque.

Article 2. Les critères d'évaluation de la sensibilité

La sécurité des systèmes d'information repose sur les quatre critères :

- **Disponibilité :** garantir la continuité du service, assurer les objectifs de performances (temps de réponse) et respecter les dates et heures limites des traitements.
- **Intégrité :** garantir l'exhaustivité, l'exactitude, la validité et la non-redondance de l'information. Éviter la modification, par erreur ou par malveillance, de l'information. S'assurer que l'application ne fait que ce qui lui est demandé.
- **Confidentialité :** réserver les accès aux données en fonction de leur niveau de classification et du niveau d'habilitation des «utilisateurs». Garantir le secret des données échangées entre deux correspondants sous forme de messages ou de fichiers.
- **Traçabilité :** vérifier le bon déroulement d'une fonction. Garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves (non-répudiation : impossibilité pour une entité de nier avoir reçu ou émis un message).

Article 3. Le niveau de sensibilité

Pour obtenir un classement de la donnée on attribue une valeur numérique de 0 à 4 à chaque critère de sécurité (disponibilité, intégrité, confidentialité et preuve) de la donnée. Le chiffre 4 est le plus élevé et 0 le plus bas.
Les mesures de protection des informations par critères de sécurité peuvent être les suivants :

- **Disponibilité :** duplication, sauvegarde, secours, machine à tolérance de pannes…
- **Intégrité :** certification, contrôle d'accès, scellement...
- **Confidentialité :** contrôle d'accès, chiffrement...
- **Traçabilité (preuves) :** logs, traçage, authentification, accusés de réception, reconstitution de la donnée, pistes d'audit...

Article 4. Le niveau de confidentialité

Quatre niveaux de confidentialité sont retenus :

- la mention «NC» (Non Classifié) s'applique uniquement aux informations qui peuvent circuler **librement à l'extérieur** du ministère, et ne justifient donc pas de protection particulière ;
- la classe de confidentialité «C1» (Usage Interne), applicable par défaut, regroupe les informations qui peuvent **circuler librement à l'intérieur du ministère** ;
- la classe «C2» (Diffusion Restreinte) s'applique aux informations qui ne doivent être communiquées (y compris à l'intérieur du ministère) qu'aux personnes directement concernées et identifiées précisément. La divulgation de ces informations pourrait nuire au fonctionnement d'une entité ainsi qu'au bon déroulement d'un projet ou d'une mission ;
- la classe «C3» (Secret) est réservée aux rares informations dont la divulgation à des personnes non autorisées pourrait porter atteinte aux intérêts stratégiques de l'organisation, à sa sécurité voire à l'existence même de l'organisation ou de l'une de ses entités. Du fait

des obligations et des contraintes créées par l'utilisation de la classification «C3», il convient d'en faire approuver son usage dossier par dossier au niveau approprié dans chaque direction.

Article 5. Typologies des menaces

Trois types de menaces sont répertoriés :

- malveillance (vol, sabotage matériel, fraude, intrusion, virus, indiscrétion, divulgation, copie illicite...) ;
- accidents (incendie, dégât des eaux, pannes, événement naturel, catastrophe, électricité, transmission...) ;
- erreurs (erreur d'utilisation, erreur de conception).

Les menaces s'appréhendent à tous les niveaux de l'exploitation de la donnée à savoir au niveau du :

- stockage (fichiers, base de données, sauvegardes...) ;
- traitement (applications, système d'exploitation...) ;
- flux (transport, liaison, réseau, routage...).

Article 6. Gravité du risque

Les risques s'apprécient selon une échelle de cinq niveaux de 0 à 4.

4 Stratégique ou Vital	Tout événement susceptible d'**entraîner l'arrêt immédiat ou rapide d'une activité.**
3 Critique ou Important	Tout événement pouvant entraîner **l'arrêt d'une partie d'une activité.**
2 Sensible	Tout événement susceptible **d'occasionner des dommages significatifs.**
1 Faible	Tout événement pouvant générer une nuisance organisationnelle faible, interne au domaine considéré mais peu gênante pour «l'utilisateur».
0 Nul	Tout évènement ayant un impact non significatif.

Article 7. Croisement de la sensibilité des biens, des menaces et de la gravité des risques

La classification d'une information doit être évaluée afin de prendre en compte tout à la fois :

- la sensibilité du bien ;
- la réalité des menaces qui pèsent sur ce bien ;
- la gravité des risques qui sont liés à ces menaces.

Cette évaluation est réalisée par un croisement de ces trois facteurs sur la base du tableau présenté ci-dessous.

gravité du risque	menaces : impossibilité de vérifier ou de prouver la qualité d'une information ou d'un traitement en cas de controverse	indisponibilité dans les délais requis pour une exécution d'une opération	modification erronée ou illicite	divulgation ou perte
4 Tout événement susceptible d'entraîner l'arrêt immédiat ou rapide d'une activité	**stratégique ou vital**	**stratégique ou vital**	**stratégique ou vital**	**secret (C3)**
3 Tout événement pouvant entrainer l'arrêt d'une partie d'une activité	**critique ou important**	**critique ou important**	**critique ou important**	**diffusion restreinte (C2)**
2 Tout événement susceptible d'occasionner des dommages significatif	**sensible**	**sensible**	**sensible**	**diffusion restreinte (C2)**
1 Tout événement pouvant générerune nuisance organisationnelle faible. Interne au domaine considéré et peu genante pour l'utilisateur	**faible**	**faible**	**faible**	**usage interne (C1)**
0 Tout événement ayant un impact non significatif	**nul**	**nul**	**nul**	**non classifié (NC)**
	preuve	**disponibilité**	**intégrité**	**confidentialité**
	critères d'évaluation de la sensibilité			

Cette table montre qu'une **information jugée critique** en termes de **confidentialité**, dont la **menace de divulgation** est à craindre, dont le risque pourrait occasionner des **dommages significatifs**, devra être classifiée **diffusion restreinte (C2)**.

En revanche, une **information jugée elle aussi critique** en termes de **confidentialité**, dont la divulgation entraînerait **l'arrêt immédiat ou rapide d'une activité**, mais dont la divulgation n'est pas à craindre car elle n'est **pas réalisable** dans l'environnement d'utilisation de cette information, sera **Non Classifiée (NC)**.

3.3 Protection des informations

Article 1. Principes généraux

- Les critères de diffusion interne des informations doivent être connus afin d'en limiter l'accès aux seules personnes autorisées.
- Les copies d'informations doivent être faites dans le respect de la réglementation en vigueur.
- Les conditions de conservation et de destruction des informations doivent être définies.

Les règles de protection de l'information sont déterminées en fonction de leur sensibilité. C'est pourquoi, la classification des informations permet de définir le moyen de communication et les règles de protection associées.
La classification de l'information est assurée par l'auteur. Le degré de sensibilité permet aux personnes qui les reçoivent et qui les traitent de suivre les consignes de sécurité accordées à l'information.

Article 2. La gestion de document classifié

Dès la phase d'élaboration d'un document, l'émetteur doit définir son niveau de sensibilité et appliquer la classification en utilisant les termes définis par la méthode de classification.
L'archivage d'un document est sous la responsabilité d'un dépositaire.
Le dépositaire est une personne nommément désignée pour assurer la conservation, la sécurité de l'archivage ainsi que la diffusion contrôlée auprès des demandeurs autorisés.
La procédure d'archivage doit être validée par le RSSI auquel est rattaché le dépositaire.
Les documents originaux ont une valeur juridique qui doit être pris en compte dans les procédures d'archivage.
Les documents (les mots de passe administrateurs, …) doivent être rangés dans un coffre blindé à combinaison si le niveau de classification est «C3» ou «C4» en confidentialité.
Les documents ainsi que tous les moyens de reproduction doivent

être placés dans une zone de confiance sous contrôle.
Les documents originaux classifiés au niveau «C2» ou plus en disponibilité ou en preuve doivent être conservés dans un local différent où sont classées les copies.
Le local d'archivage doit être physiquement protégé.

Article 3. Protection des informations stockées ou traitées

Les mesures de protection à mettre en œuvre pour protéger les informations stockées ou traitées sur des postes de travail sont déterminées en fonction de leur sensibilité et de leur niveau de classification.
La responsabilité de l'équipement matériel et logiciel de chaque poste de travail est confiée à une personne chargée de maintenir et contrôler la conformité de chaque poste de travail à la politique de sécurité du site.
Un poste de travail manipulant des informations sensibles (à partir de «C2»), devra être confié à un service spécialisé distinct du service bureautique classique.
Le stockage des informations en local doit être limité au profil d'un stockage sur une unité distante bénéficiant des capacités de sauvegarde, de secours et de protection élevées.
L'information stockée doit être exempte de virus. Pour cela chaque poste de travail doit être équipé d'un antivirus régulièrement et automatiquement mis à jour.

Les données stockées doivent être protégées contre les risques de divulgation et d'altération de la manière suivante :

- les fichiers doivent être chiffrés sur leur support à partir du niveau de classification «C3» en confidentialité ;
- les fichiers doivent être signés à partir du niveau de classification «C3» en intégrité ;
- les fichiers (logs, pistes d'audit, …) dont le niveau de classification est supérieur ou égal à «C3» en preuve doivent être archivés.

Les postes nomades doivent être considérés sensibles et doivent être à ce titre équipés notamment des dispositifs suivants :

- un système de contrôle d'accès individualisé réalisé à partir d'un support d'authentification tel que : clé USB, carte à puce, «token» (jeton), etc. ;
- un mécanisme interdisant le «démarrage» d'un poste de travail à partir d'un composant externe ;
- un système de détection d'inactivité et de désactivation des ressources du poste de travail ;
- un moyen de chiffrement des données.

Des précautions doivent être prises pour gérer la perte ou l'oubli des moyens de protection mis en œuvre. Tels qu'une sauvegarde du support d'authentification, une procédure de secours pour changer les mots de passe ou code confidentiel de la carte, le séquestre des clés de chiffrement / déchiffrement, …
Bien que l'objectif à moyen terme soit de généraliser la mise en place de l'authentification forte, les applications utilisant encore les mots de passe comme moyen d'authentification doivent appliquées les règles suivantes :

- le mot de passe doit être renouvelé au minimum tous les six mois ;
- le mot de passe doit comporter au moins sept caractères formant une combinaison de caractères spéciaux et de lettres alphanumériques ;
- les mots de passe doivent être conservés chiffrés.

4. Principes de sécurité liés aux systèmes informatiques et de télécommunications

4.1 Protection des systèmes informatiques et de télécommunications

Article 1. Principes Généraux

- La mise en place des moyens et des procédures de sécurité physique tiendra compte des contraintes spécifiques des différents établissements du ministère.

- Les mesures de protection adéquates doivent être mises en place avant l'installation des systèmes informatiques.
- Les mesures de protection des systèmes d'information et de télécommunications doivent être régulièrement évaluées.

Il est nécessaire de protéger physiquement le système d'information contre des évènements volontaires ou accidentels préjudiciables tels que : vol, destruction de support, etc., et également contre les risques dits «naturels» : incendie, dégâts des eaux, une coupure d'énergie, du circuit de climatisation, la foudre, etc.
Les ressources sensibles, donc requérant une protection renforcée, sont protégées en fonction de leur sensibilité et des risques encourus par les moyens physiques adéquats.

Article 2. Responsabilités

La sécurité physique est placée sous la responsabilité du service d'exploitation. Elle comprend :

- l'accès aux locaux d'exploitation ;
- la protection physique des équipements ;
- l'accès aux câblages du réseau ;
- les mesures de sécurité contre les intempéries, incendies, etc.

4.2 Gestion des systèmes informatiques et de télécommunications

Article 1. Principes Généraux

- Les systèmes d'information et de télécommunications sont placés dans des zones de confiance, fonction du niveau de sécurité des informations manipulées.
- La zone de confiance à laquelle appartient un système informatique et de télécommunications doit être connue pour en permettre l'installation.
- Les protections nécessaires à chaque zone doivent être définies.

- Une zone de confiance est une zone dans laquelle tous les «utilisateurs» et toutes les ressources correspondent à un même niveau de confiance, c'est à dire respectant les mêmes règles de sécurité.

Le cloisonnement par zones doit permettre de limiter l'accès aux systèmes informatiques les plus sensibles:

- les traitements des incidents de sécurité doivent être maîtrisés pour éviter la propagation du sinistre ;
- les accès aux systèmes d'information et les types de flux doivent faire l'objet de journalisations techniques permettant un contrôle a posteriori ;
- le niveau de détail des informations ainsi collectées doit être suffisant pour traiter les actions illicites. La surveillance de ces traces doit être régulière ;
- les systèmes informatiques utilisés hors de leur zone de sécurité doivent faire l'objet de protections spécifiques, et doivent être contrôlés avant leur remise en place.

Article 2. Définition des zones de confiance du ministère

Un espace de confiance est un espace dans lequel est défini un niveau de sécurité. Un espace de confiance a un responsable identifié.
L'existence de cet espace et les moyens mis en œuvre, sont validés au niveau local et national selon le niveau de recouvrement de l'espace considéré.
Afin de restreindre les risques de propagation d'une menace sur l'ensemble du Système d'Information de l'Éducation nationale, le réseau est découpé en zones de confiance sur lesquelles s'appliquent les mesures de nature :

Organisationnelle

- tout composant technique - matériel ou logiciel - connecté au Système d'Information de l'Éducation nationale doit obligatoirement être rattaché à une zone de confiance ;
- tous les flux de données susceptibles d'être établis entre l'un des composants d'une zone de confiance et un composant extérieur à

celle-ci, doivent être identifiés, déclarés et contrôlés. Chaque lien existant doit obligatoirement avoir fait l'objet d'une déclaration préalablement à sa mise en service.

Opérationnelle

- les flux de données échangés aux interfaces d'une zone de confiance doivent être maîtrisés ;
- les flux échangés entre Internet et une zone de confiance doivent obligatoirement passer par une plate- forme dédiée et homologuée notamment pour ce qui concerne le domaine scolaire.

Le système d'information et de télécommunications de l'Éducation nationale, dans la sphère scolaire, est structuré en cinq zones de confiance.

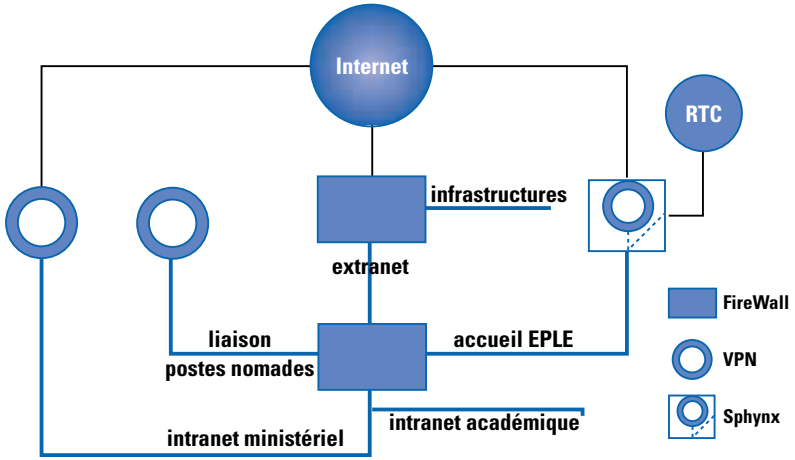
Il est nécessaire de connaître très précisément la zone de confiance dans laquelle le système d'information est mis en œuvre afin d'appliquer les mesures de sécurité appropriées.
Chaque zone de confiance est définie comme un regroupement logique de composants techniques qui permet d'identifier précisément un périmètre de protection réaliste tant en terme de responsabilité que d'infrastructure organisationnelle ou technique.

1. Zone Intranet site (ce qui est propre à chaque site)	La zone Intranet de site peut s'étendre sur plusieurs localisations géographiques. Elle s'applique aux échanges sur les réseaux locaux et les interconnexions de réseaux au sein d'une unité administrative reconnue telle qu'un rectorat, une inspection académique, un lycée, un collège, etc.
2. Zone Intranet étendu (ce qui fédère les services académiques et centraux)	La zone Intranet étendu concerne les échanges entre les services de l'Éducation nationale (rectorats, inspections académiques, administration centrale).
3. Zone Intranet adémique (ce qui rassemble les établissements et les services académiques)	La zone Intranet académique concerne les échanges entre les services académiques et les établissements ainsi que les échanges des établissements entre eux.

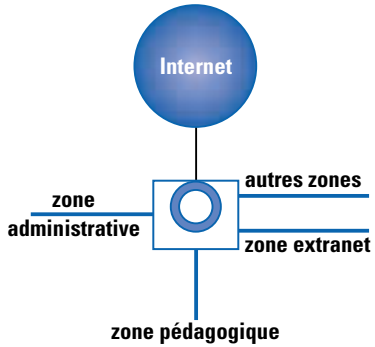
4. Zone Intranet académique étendue (ce qui prend en compte la pluralité des lieux de travail)	La zone Intranet académique étendue concerne les personnels exerçant leurs fonctions sur un site isolé ou travaillant à domicile et autorisés à accéder aux systèmes d'informations des service et / ou établissements.
5. Zone Extranet (ce qui ouvre le système d'information aux partenaires)	La zone Extranet concerne les échanges entre les services de l'Éducation nationale et les autres services de l'état ou d'autres établissements «étrangers».

Le verrouillage des zones de confiances n'est activable que par les Correspondants de Sécurité sur demande expresse du RSSI.
Les 2 schémas ci-après présentent le cadre général d'application de ces prescriptions au niveau d'un Rectorat et d'un EPLE. Les dénominations des zones apparaissent sous leur forme usuelle afin de favoriser la liaison entre les concepts présentés au sein de ce paragraphe et les pratiques du MENESR.

exemple d'organisation du réseau des services académiques en zones de confiance



exemple d'organisation d'un réseau EPLE en zones de confiance



Article 3. Principe d'architecture sécurisée

Alinéa a. Principes Généraux

«La solidité d'une chaîne est celle du maillon le plus faible» : renforcer cette chaîne nécessite donc de disposer d'une méthode et de principes conduisant à la conception et à l'assemblage de maillons homogènes.
Les principes d'architecture et de sécurité ont pour but de structurer les systèmes d'information pour répondre à deux objectifs :

- faciliter la communication au sein de la communauté éducative ;
- protéger l'information contre des accès illicites ou illégitimes.

Son fondement se trouve dans l'application de trois principes fondamentaux présentés aux alinéas b, c et d.

Alinéa b .Principe de réduction du risque

L'atteinte à la sécurité de l'un des quelconques constituants du système d'information ne doit pas conduire à mettre en péril la sécurité de l'ensemble des services offerts par celui-ci. Les mesures de protection ont pour objectif prioritaire de circonscrire le risque en limitant la propagation d'un éventuel sinistre au delà d'un périmètre de protection prédéfini.
Les règles de confinement répondent au principe de réduction du risque et sont mises en œuvre dans les zones de confiance.

Alinéa c. Principe de proportionnalité

L'effort de protection est proportionnel aux risques encourus. Les composants du système d'information sont regroupés afin de former plusieurs zones de confiance. La nature et l'organisation de ces regroupements doivent favoriser la mise en évidence de frontières et de liens de communication placés sous la tutelle d'une autorité neutre et centrale.

Alinéa d. Principe de subsidiarité

La mise en œuvre des mesures de sécurité s'appuie sur l'organisation interne des entités opérationnelles en charge de l'exploitation. La sécurité des réseaux n'est donc pas l'œuvre d'une instance centrale mais le résultat d'une contribution de l'ensemble des services d'exploitation.

Alinéa e. Isolement des zones de confiance vis-à-vis de l'extérieur

L'Éducation nationale est une institution répartie sur plusieurs sites. L'administration centrale, les rectorats et les inspections académiques pour les services de l'État, les établissements scolaires, établissements du supérieur et enfin, les écoles.
On retrouve dans le système d'information et de communication les niveaux nationaux, académiques, départementaux et établissements.
L'unité du système d'information de l'éducation nationale est entre autre dûe au respect des mêmes règles d'inter-opérabilité sur chaque site, le plus couramment avec les mêmes applications (projets nationaux).
La normalisation des infrastructures, notamment en ce qui concerne la sécurité, est donc un élément garant du bon fonctionnement d'un système d'information et de communication prenant en compte la globalité de l'Éducation nationale.

Ce principe a pour objectif :

- de limiter les conséquences d'une intrusion interne ;
- de protéger le réseau contre les attaques externes ;
- de protéger les «utilisateurs» contre des erreurs d'administration ou des abus de droits.

Alinéa f. Zones de communication avec l'extérieur

L'accès à une zone de confiance depuis l'extérieur n'est autorisé qu'après une authentification de «l'utilisateur» et sous réserve que d'autres personnes ne puissent emprunter la liaison ainsi établie.

Les zones de confiances sont protégées de l'extérieur par trois types de mesure :

- filtrage des accès «entrants» (initialisés de l'extérieur pour accéder à l'intérieur d'une zone de confiance) ;
- filtrage des accès «sortants» (initialisés à l'intérieur d'une zone de confiance vers l'extérieur) ;
- filtrage du contenu des échanges

Ces filtrages prennent en compte les moyens physiques, l'origine, la destination et le type de flux de la communication.

Le filtrage du contenu met en œuvre systématiquement :

- un contrôle anti-virus ;
- un système de détection des tentatives d'intrusion (IDS).

Alinéa g. Accès au réseau Internet initialisés depuis une zone de confiance

L'accès à Internet depuis une zone de confiance n'est autorisée qu'après authentification de «l'utilisateur».
Les sites déclarés illicites sont filtrés et les informations de reporting sont fournis aux PJR sur l'utilisation de l'Internet.

5. Principes liés à l'organisation de la sécurité

5.1 Structure de la sécurité

Article 1. Principes généraux

- La structure de sécurité est l'organisation mise en place pour la gestion des différentes composantes de la sécurité et de leurs

évolutions ; elle implique un partage des responsabilités entre les différents niveaux, à savoir :
- le niveau décisionnel
- le niveau de pilotage
- le niveau opérationnel.

Les chaînes de responsabilité doivent réagir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

Article 2. La Personne Juridiquement Responsable (PJR)

L'autorité hiérarchique d'une entité est responsable de la sécurité des systèmes d'information existants ou à venir, exploités par et pour elle-même. Ainsi, elle doit mettre en place une organisation chargée de l'application des mesures de sécurité et du contrôle de son efficacité.
Elle est personnellement responsable de la définition et de l'application de la politique de SSI d'un organisme.
Par convention, l'autorité hiérarchique sera appelée «Personne Juridiquement Responsable» ou PJR.
Le recteur d'académie, le président d'université, l'inspecteur d'académie, l'inspecteur de l'Éducation nationale chargé de circonscription du premier degré, le chef d'établissement, le directeur d'établissement ou toute autre autorité d'entité composant le système éducatif sont autant de «Personnes Juridiquement Responsables» en charge de la politique de sécurité des systèmes d'information de leur sphère de responsabilité.

Pour exercer cette responsabilité, l'autorité hiérarchique doit s'appuyer sur les Responsables de la Sécurité des Systèmes d'Information.

Article 3. Le Responsable de la sécurité des systèmes d'information (RSSI)

Pour les services, les EPLE et les grands établissements, le Responsable de la Sécurité des Systèmes d'Information est nommé par la «Personne Juridiquement Responsable».

À ce titre, le Responsable de la Sécurité des Systèmes d'Information conseille la «Personne Juridiquement Responsable» en matière de sécurité des systèmes d'information.

Les missions principales du RSSI sont les suivantes :
- constituer et coordonner un réseau interne de correspondants de sécurité ;
- mettre en place les plans de sécurité adaptés aux établissements et aux services, en cohérence avec le Cadre Commun de la Sécurité des Systèmes d'Information ;
- organiser le référencement des sites dangereux ou illicites au niveau de l'académie et assurer la mise à jour des dispositifs de filtrage en conséquence ;
- contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels ;
- informer et sensibiliser les «utilisateurs» du système d'information aux problématiques de sécurité ;
- améliorer la SSI par une veille technologique active ainsi que par une participation aux groupes de réflexion ad hoc ;
- assurer la coordination avec les différents organismes concernés.

Son périmètre d'intervention pourra couvrir plusieurs entités de nature identique, bassin ou secteur scolaire pour les établissements scolaires par exemple, ou, groupement de laboratoires de recherche ayant en commun les mêmes moyens de sécurité.

A minima, l'activité du RSSI s'exerce :
- au sein du rectorat avec un champ d'intervention élargi aux autres services académiques et établissements scolaires ;
- au sein des établissements d'enseignement supérieur ;
- à l'administration centrale.

Pour assurer pleinement toutes les composantes de sa mission, le RSSI s'appuie sur une chaîne de Correspondants de Sécurité qu'il organise et dont il est le référent.

Article 4. Les Correspondants de Sécurité

Sous l'autorité de la PJR et l'appui nécessaire du RSSI, les Correspondants de Sécurité sont chargés de la mise en œuvre de la sécurité au sein d'une entité donnée. Ils ont une qualification informatique de niveau administrateurs systèmes et réseaux ou, à défaut, des compétences reconnues en la matière. Leur nombre peut varier selon la nature et la taille de l'entité dans laquelle ils évoluent.
Les Correspondants de Sécurité mettent en oeuvre les règles générales d'exploitation, consignées dans le carnet de sécurité des systèmes d'information, pouvant être complétées par des mesures liées aux spécificités de l'entité.
Chaque Correspondant de Sécurité doit être désigné. Sa prise de fonction est accompagnée de la prise de connaissance d'une charte nationale «administrateurs» par laquelle il est informé de ses droits et devoirs. Dès lors, il s'engage à respecter cette charte qui est annexée au règlement intérieur de l'entité.
Tout Correspondant de Sécurité doit être identifié et associé à la politique académique de sécurité.
Pour les entités les plus importantes, l'identification des correspondants est réalisé par système ou par domaine (GRH, concours, …).

5.2 Continuité de contrôle de la sécurité

Voir aussi : **chapitre 6 - 6.6 - (Article 3.** Tableaux de bords et Pilotage de la sécurité)

Le contrôle de la sécurité doit être exercé régulièrement et donc prévu dans le plan de charge de tous les niveaux de responsabilités.

Les activités de contrôle doivent s'appuyer sur des principes déclinés de la manière suivante :

Au niveau opérationnel
- surveillance des ressources en continu par les équipes techniques ;
- vigilance permanente des «utilisateurs» ;
- traitement des incidents au travers d'un processus de qualification, d'alerte et de résolution des incidents de sécurité.

Au niveau décisionnel
- pilotage de l'effort de sécurisation ;
- suivi des tableaux de bords de sécurité.

Au niveau des réseaux d'expertise de la sécurité
- veille technologique de sécurité permanente et prévention des incidents ;
- capitalisation des savoir-faire et des pratiques propres à la sécurité.

6. Principes de sécurité liés au cycle de vie du système d'information

6.1 Spécification pour le développement du système d'information

Article 1. Principes généraux

Une méthode de développement des applications approuvées doit être utilisée afin de garantir la sécurité du système d'information.
La sécurité doit être prise en compte dès le départ qu'il s'agisse de projets d'infrastructure (réseaux, systèmes, …) ou de projets de développement d'applications.

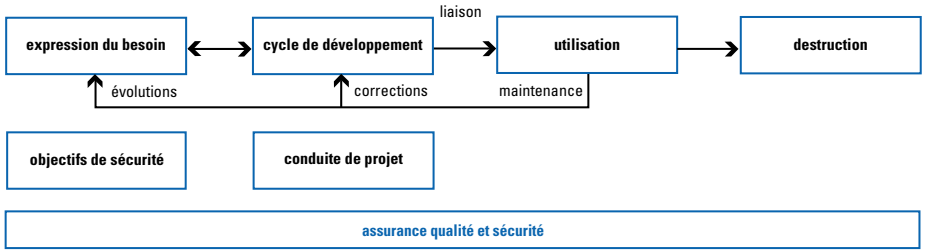
Les besoins de sécurité sont analysés selon deux axes :
- développement : les besoins de protection de l'information qui peuvent conduire à la création d'un espace sécurisé pour la réalisation ;
- exploitation : les besoins de continuité de l'activité qui impliquent l'élaboration d'un plan de secours.

Le cycle de vie «classique» d'un système d'information peut se décomposer en 4 phases principales :

- l'expression du besoin : phase d'élaboration des spécifications ;
- le cycle de développement : phases de production au sens large ;
- l'utilisation : phases de mise en fonctionnement, d'utilisation en mode nominal, et de maintenance ;
- la destruction : phases d'arrêt et de démantèlement du système.

Le schéma ci-dessous présente, dans ce contexte, les lieux d'application de la démarche sécurité.

Évaluation de la sécurité



Les objectifs de sécurité constituent une composante indispensable de l'expression des besoins. Leur formulation doit s'appuyer sur un socle méthodologique accessible aux MOA, proche des concepts habituellement employés par les MOE et en accord avec les directives interministérielles. Les outils EBIOS, PSI, et DSIS répondent, moyennant des adaptations contextuelles, à ces impératifs.

Bien que les phases de détermination des objectifs et d'évaluation de la sécurité s'étendent essentiellement sur la partie amont du cycle de vie d'un projet, les rétroactions engendrées par les actions de maintenance conduisent à nuancer cette approche :

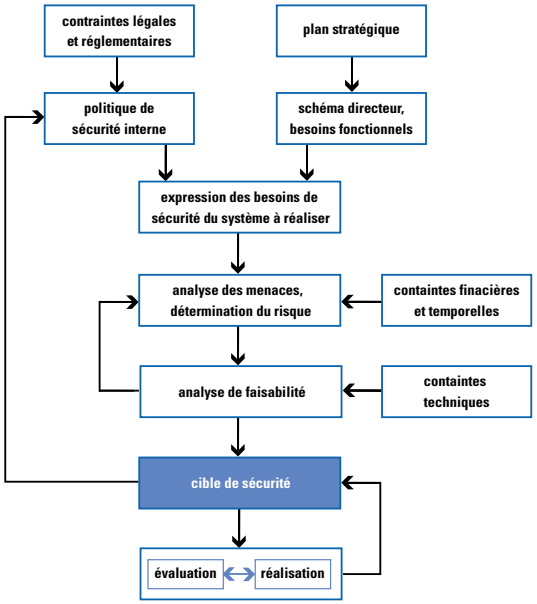
- les maintenances correctives amenant à revenir sur la phase d'évaluation ;
- les maintenances évolutives imposant de réviser les objectifs de sécurité ainsi que la phase d'évaluation.

D'autre part la fin du cycle de vie d'un produit, notamment lors des opérations de reprise de données et d'archivage impose un suivi approprié en terme de sécurité.
C'est ainsi que **la notion d'assurance sécurité s'applique à l'intégralité du cycle de vie** et nécessite à l'instar de l'assurance qualité des **outils de suivi et de traçabilité** qui seront **mis en œuvre pour l'ensemble des projets** des systèmes d'information du MENESR.

La cible de sécurité du système à concevoir est définie à partir de 4 entrées principales :

- les contraintes légales et réglementaires ;
- le plan stratégique ;
- des contraintes financières et temporelles ;
- des contraintes techniques.

Celles ci sont intégrées en amont du projet ou lors de phases propres à l'expression du besoin. Il convient de souligner l'importance de la confrontation des résultats de l'analyse des menaces et de l'analyse de faisabilité ainsi que les rétroactions qui interviennent entre ces processus.



Article 2. Pilotage de la sécurité dans le cycle de vie des projets

Tout projet doit avoir un volet sécurité totalement intégré à son cycle de vie : conception, réalisation, test et validation, homologation, mise en production, maintenance et fin de vie.

Un Dossier de Sécurité mesurant l'impact du projet sur l'activité et spécifiant les besoins de sécurité doit être élaboré systématiquement. La décision de créer un espace sécurisé pour la réalisation du projet est prise en fonction de la sensibilité exprimée.

L'objectif du Dossier de Sécurité est de répondre aux questions :
- quels risques encourt le système d'information mis en place ?
- quelles solutions doivent être mises en place ?
- quels sont les risques non couverts ?

Les risques non couverts, (ou risques résiduels), doivent faire l'objet d'une validation de la part des directions opérationnelles ou de la PJR afin de vérifier qu'ils demeurent acceptables au regard de la politique de sécurité globale.

Le Dossier de Sécurité décrit les besoins du système tant en terme fonctionnel que de sécurité. Les besoins fonctionnels du système recouvrent tous les aspects du système en rapport avec les environnements : techniques (client, serveur et réseau), humains («utilisateur» et «administrateur») et applicatifs (application et services).

Les besoins de sécurité sont déclinés en terme de disponibilité, intégrité, confidentialité et traçabilité. Ces différents besoins sont explicités, chaîne de liaison par chaîne de liaison. Chaque flux échangé, qu'il soit opérationnel ou d'administration, est défini qualitativement et quantitativement de manière exhaustive.

L'évaluation de la gravité d'un sinistre ou dysfonctionnement se mesure à l'aide de chacun des critères énoncés précédemment.

Article 3. Création d'un espace de confiance pour la protection de l'information dans les projets

L'espace sécurisé peut être décidé par la maîtrise d'ouvrage lorsque les données ou les ressources du projet sont classifiées au niveau «C3» ou plus.
Tous les projets ne nécessitent pas la création d'un espace sécurisé. Le Dossier de Décurité permet de répondre à cette question.

Article 4. Sécurité des développements informatiques et de la maintenance applicative

Les environnements (matériel, logiciel) de développement informatique (réalisation, validation, intégration, maintenance) et exploitation doivent être séparés (i.e sur des machines différentes et sur des supports de données différents).
Les équipes de développements n'ont pas de droit d'accès aux environnements de production.

Les données de tests utilisées par les développeurs pour la qualification de leurs travaux ne doivent en aucun cas provenir des environnements de production.

Le chef de projet avec l'aide de la maîtrise d'ouvrage réalise un plan de test qui doit obligatoirement être appliqué avant la mise en production. Ce principe s'applique à tout achat sur rayon, création ou modification de logiciel, progiciel ou application.
Les changements de version doivent faire l'objet des mêmes contrôles et de la même rigueur que les développements. Il est nécessaire de prévoir systématiquement le retour à la situation antérieure afin de traiter les cas où le changement ne serait pas opérationnel et/ ou des fonctionnalités auraient régressé.
Les applications doivent être accompagnées d'une documentation (manuel utilisateur, dossier d'exploitation, dossier de maintenance, ...) qui doit être mise à jour et conservée en lieu sûr.

Article 5. Cadre méthodologique «Sécurité et Développement»

Le cadre méthodologique «sécurité» reprend les grands principes de conception et de développement des SI. Les spécifications de sécurité sont étroitement associées aux niveaux de conception : système d'information, sous-système et composant.
La gestion en configuration des documents relatifs aux aspects sécurité est traitée de la même manière et avec la même rigueur que les autres produits des méthodes de conception & développement.

L'ensemble documentaire se compose de :
- la Cible De Sécurité (CDS) ;
- le Plan d'Assurance Sécurité (PAS) ;
- le Dossier des Tests de Sécurité (DTS) - qui peut faire partie du dossier des tests ;
- le Dossier d'Analyse des Vulnérabilités (DAV) ;
- les Manuels De Sécurité «utilisateur» et «administrateur» (MDS).

Rappelons que la Cible de Sécurité (CDS) contient notamment une politique de sécurité technique (ou un argumentaire de sécurité pour un produit) et la spécification des fonctions de sécurité.
Au début du projet on considère que l'on dispose d'une ébauche de la Cible De Sécurité* ainsi que d'une analyse préliminaire des menaces applicables au système ou au produit à réaliser.
Par ailleurs, on suppose qu'il existe un Dossier de Développement du Système (DDS).
(* Si la décision de faire évaluer un système est prise après sa réalisation, la Cible De Sécurité sera rédigée une fois le système disponible. Il est alors probable que le système ne pourra pas prétendre à un niveau d'évaluation de sécurité élevé ; en l'absence de possibilité de correction d'erreurs éventuelles, le risque d'échec de l'évaluation est très important.)

La DCSSI a élaboré un guide pour le Développement de Systèmes d'Information Sécurisés (DSIS) afin d'aider les concepteurs à maîtriser la sécurité au cours de leurs projets et à réaliser des systèmes

sécurisés susceptibles de remplir les conditions nécessaires à une évaluation de sécurité. Cet outil est disponible sur le site **http://www.ssi.gouv.fr** dans les rubriques de méthodologie.

Article 6. Les environnements d'exploitation

Les environnements d'exploitation ne peuvent pas être utilisés pour des expérimentations ou comme des environnements de développement.
Les services d'exploitation doivent disposer de trois types d'environnement : développement, homologation et production. Chacun de ces environnements est indépendant et cloisonné (habilitations, exécutables et données distincts).
La sécurité de l'exploitation s'appuie sur une séparation de fonction.
Les moyens informatiques et de télécommunications sont exploités par des services identifiés et spécialisés.
Une application ne peut être exploitée par les personnels qui réalisent le développement ou la maintenance du système.
Les exploitants ont la responsabilité des infrastructures matérielles.

Le service d'exploitation

- tient à jour la nomenclature avec les numéros de version des composants logiciels, des configurations en exploitation ;
- effectue le suivi des correctifs logiciels dans l'environnement d'homologation avant la mise en exploitation ;
- s'assure de la mise en place des procédures de sauvegarde et de restauration permettant d'assurer la continuité opérationnelle ;
- désigne un Correspondant de Sécurité chargé du suivi et de la mise en œuvre des plans de secours.

Tout équipement, machine ou poste de travail doit être supervisé par un service d'exploitation identifié.

Le service d'exploitation organise en fonction du contrat de service

- l'accueil et assistance à «l'utilisateur» ;
- les informations remontées en cas d'incident ;
- les plages d'astreinte et les arrêts programmés ;
- le taux de disponibilité du système.

Article 7. Prestations de services externes

Les prestations de services externes sont soumises au respect du Cadre Commun de la Sécurité des Systèmes d'Information ainsi qu'a toute mesure contractuelle jugée nécessaire par le RSSI.
Les obligations des parties en matière de sécurité doivent être consignées dans un document spécifique annexé aux CCTP.
Le Cadre Commun de la Sécurité des Systèmes d'Information s'applique aux prestations de services sous-traitées ou externalisées. Si des adaptations sont nécessaires, elles doivent être validées par le RSSI.

La rédaction d'un contrat d'externalisation ou de sous-traitance doit de manière non exhaustive stipuler :

- le respect du Cadre Commun de la Sécurité des Systèmes d'Information ;
- la possibilité de faire un audit sur la fourniture ;
- la propriété intellectuelle et industrielle ;
- la protection contre les actions de contrefaçon ;
- la clause de confidentialité ;
- le niveau de service attendu ;
- la clause de pénalité.

6.2 Autorisation pour l'utilisation du système d'information

Article 1. Principes Généraux

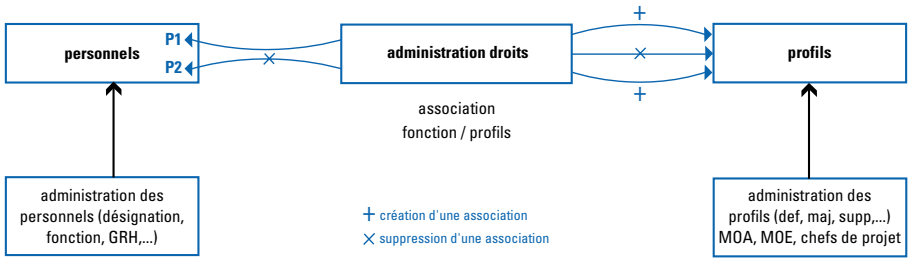
- À chaque fonction, justifiant d'un accès aux systèmes d'information, correspond un profil d'autorisation associé.
- Une personne peut être rattachée à plusieurs profils d'accès aux systèmes d'information. Chaque profil étant représentatif d'une de ces fonctions.
- L'administration des privilèges associés à un profil doit être définie et faire l'objet d'évaluations régulières.
- Le rattachement d'une personne à des profils et aux privilèges

associés doivent être mis à jour à chaque changement dans les fonctions des personnes.
- Une identification est requise pour accéder aux systèmes d'information. Un profil de type anonyme, sans identification, peut être autorisé pour l'accès aux données classées ordinaires.
- «L'administrateur» des profils doit être informé de tout changement ou cessation de fonctions.

Article 2. Principes de gestion des habilitations

L'accès logique est attribué selon une procédure d'habilitation qui s'appuie sur une connaissance directe de «l'utilisateur».
L'habilitation engage la responsabilité de chaque «utilisateur» par l'observation des règles suivantes :

- les «utilisateurs» du système sont identifiés individuellement, de manière unique et normalisée ;
- le code confidentiel est le moyen de vérifier l'identification fournie par une personne. Il est tenu secret vis-à-vis des tiers. Il est interdit de pré-enregistrer des procédures de connexion comportant le code confidentiel.



Article 3. Sécurité logique et contrôle d'accès aux applications et informations

Alinéa a. Attribution et gestion des droits

La gestion des droits par profils est nécessaire pour toutes les applications et tous les systèmes.

Le principe repose sur l'affectation de droits à un profil puis l'attribution de profils à une ou plusieurs personnes.
Une gestion laxiste des droits accordés conduit à introduire des failles dans le système de contrôle d'accès qui ne peuvent être corrigées par les mécanismes d'authentification. La gestion des droits doit être rigoureuse pour ne pas fragiliser les services d'authentification.
La responsabilité de la définition des droits relève de la MOA. La gestion des associations profils de droits / personnes est de la responsabilité d'un «administrateur» préalablement identifié.
Chaque «utilisateur» est doté d'attributs qui déterminent le niveau d'information qui lui sont accessibles ainsi que ses droits.
Le processus d'attribution et de gestion des droits doit être auditable et faire l'objet d'un contrôle périodique qui doit apparaître dans le tableau de bord de la sécurité.

Alinéa b. Processus d'identification et d'authentification

L'authentification est facteur clé du contrôle d'accès. De sa qualité et de sa robustesse dépendent la protection du système d'information contre des accès illicites. L'objectif est de généraliser l'authentification forte pour autoriser l'accès aux systèmes d'information.

Authentification forte

L'objectif est de généraliser l'authentification forte des «utilisateurs». Pour cela «l'utilisateur» possèdera d'un dispositif dédié (clé USB, carte à puce, jeton, etc.) contenant son identité numérique à partir de laquelle les mécanismes d'authentification seront mis en œuvre.

Authentification par mot de passe

Bien que l'objectif soit de généraliser l'authentification forte, les applications qui emploient encore les mots de passe comme moyen d'authentification doivent appliquer les règles de gestion suivantes :

- le mot de passe doit être renouvelé au moins tous les six mois ;
- le mot de passe doit comporter au moins sept caractères formant une combinaison de caractères spéciaux et alphanumériques ;
- les mots de passe doivent être conservés chiffrés.

Les transferts réseaux des mots de passe doivent tendre vers l'emploi systématisé de protocoles cryptés (recourant notamment aux protocoles ssh, scp et sft en remplacement des protocoles telnet, rcp et ftp).

Article 4. Règles s'appliquant aux «administrateurs» de systèmes informatiques

Toute action d'administration fait l'objet d'une identification et d'une authentification individualisées. Les comptes génériques ou partagés sont strictement prohibés. L'accès aux outils de l'exploitation (administration des privilèges, sauvegardes, copies, reprises à chaud, etc.) doit être limité et contrôlé.

La journalisation systématique des actions d'administration doit être effectuée.
L'accès aux données ainsi que l'utilisation des outils d'investigation doivent être limités aux stricts besoins de l'exploitation.

6.3 Exploitation sécurisée du système d'information

Voir aussi : **chapitre 6 – 6.6 - (Article 1.** Alinéa a. Plans de sauvegarde), **chapitre 4 – 4.2 - (Article 3.** Alinéa e. Isolement des zones de confiance vis-à-vis de l'extérieur)

Article 1. Principes généraux

- Les règles d'exploitation d'une application doivent être compatibles avec le niveau de sécurité qui lui a été associé.
- Tout nouveau constituant du système d'information doit être vérifié également sur le plan de la sécurité.
- Tout logiciel devra être contrôlé avant sa mise en exploitation afin de vérifier que son fonctionnement respecte les règles de sécurité en vigueur dans la zone d'installation.

Article 2. Convention de service

Une convention de service précise les engagements de l'exploitation vis-à-vis des besoins et exigences exprimés par la maîtrise d'ouvrage lors de la mise en production (application, composants d'infrastructure, etc.). Il s'agit de la conjugaison du cahier d'exploitation, du carnet de sécurité et de la politique de sécurité des systèmes d'information du site hébergeur.

Cette convention décrit le niveau de secours, la sécurité physique et logique, les tâches d'exploitation prévues et les plages d'astreinte, la disponibilité requise et les mesures conservatoires (plan de sauvegarde).

Doivent être ainsi spécifiés :
- les performances attendues en terme de disponibilité ;
- les délais de reprise sur incidents et conditions d'astreinte du personnel ;
- les modes dégradés éventuels ;
- les fréquences et les exigences pour les sauvegardes et les restaurations ;
- les modalités, contrôles et conditions d'accès des personnels d'administration et d'exploitation ;
- les exigences de confidentialité, d'intégrité et de disponibilité des données transmises, traitées et stockées ;
- les exigences relatives à la preuve : piste d'audit, logs, archivage, etc.;
- le cloisonnement éventuel.

Il est recommandé de préparer la convention de service dès la phase de conception du projet.

Les privilèges accordés aux équipes de mise en production doivent être limités pour empêcher toute modification de programmes ou de données hors du contexte de fonctionnement normal du produit. Des procédures exceptionnelles doivent toutefois être activées en cas de sinistre.

Les accès logiques aux systèmes faisant l'objet d'une classification de niveau «C2» et plus, sont soumis aux 2 règles suivantes :
- contrôle d'accès par authentification forte ;
- transmission d'information sécurisée par accès physique protégé ou l'utilisation de mécanismes cryptologiques.

Article 3. Exploitation des réseaux

Alinéa a. Principes

La sécurisation des réseaux informatiques interconnectant les différents constituants, matériels et logiciels, du Système d'Information de l'Éducation nationale repose sur des mesures organisationnelles et techniques. Toutes les règles d'architecture, générales ou spécifiques d'un espace de confiance qui ont été définies, doivent être appliquées (cf. **chapitre 4 - Article 3.** Principe d'architecture sécurisée) :
- cf. Alinéa b ci-dessous ;
- la configuration ad hoc des équipements (règles de configuration initiale, contrôle des évolutions, contrôle des configurations, contrôle d'accès aux équipements, …) de réseau ;
- le contrôle, la détection et le traitement des incidents réseaux et télécommunications ;
- la gestion de la continuité de fonctionnement (maintenance, sauvegardes, plans de reprise).

Alinéa b. Tenue d'une base d'informations sur les infrastructures réseaux, applicatives et cartographie

Le RSSI définit les limites de la zone de confiance, ainsi que les points d'inter liaison avec des réseaux sur lesquels la politique de sécurité n'est pas appliquée ou n'est pas vérifiée. Le recensement de ces informations est envoyé aux directions opérationnelles ou à la PJR.

Il est nécessaire de tenir à jour un inventaire qui comprend :
- les équipements de réseau raccordés : origine, fabriquant, modèle, fonctionnalités supportées, localisation, interfaces réseau installées et adresses IP ;

- les lignes de communication mises en œuvre : débit, protocoles, sites reliés, gestionnaires ;
- les sites reliés : correspondants, rattachements organisationnels ;
- les logiciels de base installés dans les équipements de réseau : systèmes d'exploitation, utilitaires de configuration et de gestion du réseau, scripts, etc. ;
- le plan d'adressage IP ;
- le plan de routage.

Il est nécessaire de tenir à jour également dans la base d'informations, la liste des applications et pour chacune d'elles, les protocoles mis en œuvre pour configurer les équipements de sécurité et pare feux associés.

Alinéa c. Configuration des équipements de réseau

La configuration des équipements de réseau comporte divers aspects :

- règles de configuration initiale ;
- contrôle des évolutions ;
- contrôle des configurations ;
- contrôle d'accès aux équipements.

La mise en production d'un équipement réseau ou de toute évolution ou modification de logiciel nécessite un contrôle de l'existence d'une documentation d'exploitation dans laquelle figurent les consignes de reprise et d'intervention sur incidents.
La possibilité de revenir à une situation antérieure doit toujours être garantie.

Toute intervention est préalablement soumise pour approbation au RSSI en charge du domaine, et doit être notifiée dans un journal en précisant les opérations effectuées, l'identité et la qualité de l'intervenant.

L'accès logique aux équipements de sécurité des réseaux appartenant à un espace de confiance doit respecter les points suivants :

- accès uniquement depuis la console système. Si le poste d'administration est distant, les échanges doivent être chiffrés ;
- système d'authentification forte ;
- journalisation systématique des actions d'administrations effectuées.

Alinéa d. Contrôle, détection et traitement des incidents réseaux et télécommunications

Des mesures et des analyses de performance doivent être effectuées périodiquement afin de détecter des anomalies de fonctionnement, des interruptions de service ainsi que des distorsions par rapport aux exigences des conventions de service.
Chaque point de raccordement ou de cloisonnement au réseau (zone de confiance) doit assurer un contrôle antivirus, une détection d'intrusion ou d'anomalies.
Les journaux (incidents, reconfigurations, reroutages, connexions refusées, …) doivent être analysés périodiquement. Les résultats de ces analyses doivent être communiqués régulièrement au RSSI.

Article 4. Exploitation des systèmes

La sécurité pour l'exploitation des systèmes concerne :

- la configuration des systèmes et des postes utilisateurs (règles de configuration initiale, contrôle des évolutions, contrôle des configurations, contrôle d'accès aux équipements critiques, etc.) ;
- les règles de configuration ;
- la gestion des supports et média informatiques ;
- la gestion de la continuité de fonctionnement (maintenance, sauvegardes, plans de reprise d'activité, protection antivirale, …).

Alinéa a. Tenue d'une base d'informations

Pour être en mesure d'exploiter un réseau local et les systèmes qui y sont connectés de manière sécurisée, il est nécessaire de maintenir à jour un inventaire permanent des composants de l'architecture à partir duquel il sera possible de déterminer :

- l'ensemble des applications hébergées par un système donné ;
- les systèmes qui concourent à l'exploitation d'une application.

L'inventaire alimente une base d'informations qui contient :

- le matériel raccordé au réseau : origine, fabriquant, modèle, localisation, interfaces réseau installées et adresses ;
- les logiciels de base installés : systèmes d'exploitation, SGBD, utilitaires de configuration et d'administration distante des systèmes ;
- les applications utilisées et ses groupes «d'utilisateurs».

Alinéa b. Configuration des systèmes et des postes utilisateurs

Tout système doit être dans le champ de responsabilité d'un RSSI désigné.

Toute intervention dans l'environnement de production est préalablement soumise pour approbation au RSSI en charge du domaine, et doit être notifiée dans un journal en précisant les opérations effectuées, l'identité et la qualité de l'intervenant.

Un examen des dispositifs de sécurité, voire une reconfiguration des dispositifs, doit être fait après chaque intervention.

La mise en production d'un matériel, d'un logiciel ou d'un progiciel ou de toute évolution ou modification de versions nécessite :

- un contrôle de l'existence d'une documentation d'exploitation dans laquelle figure les consignes de reprise et d'intervention sur incidents. Il est du ressort du responsable de projet de fournir le manuel d'exploitation dans lequel sont décrites les opérations d'exploitation attendues et les procédures d'incident. Dans le cas de projets sensibles, des tests de sécurité complémentaires sont réalisés par des spécialistes sur environnement d'homologation ;
- les pièces justificatives prouvant que les tests, recettes et installation dans l'environnement d'homologation ont été réalisés.

Les informations de configurations des serveurs sensibles classifiés «C3» et plus doivent être vérifiées régulièrement par une personne différente de celle ayant configurée le serveur.

Des contrôles réguliers par échantillonnage doivent être faits pour vérifier que les logiciels ont été licitement acquis.

La possibilité de revenir à une situation antérieure doit toujours être garantie.

Alinéa c. Règles de configurations

Pour parvenir à un niveau de sécurité constant et cohérent à l'échelon national, il est important de mettre en œuvre des règles de configuration techniques qui s'appuient sur les besoins de sécurité évalués par «métier» et populations «d'utilisateurs».

Une liste de règles de configuration et d'exploitation pour les systèmes et équipements utilisés, doit être réalisée en mettant en perspective les risques pris en compte. Ces règles ne peuvent couvrir tous les environnements ni tous les cas d'utilisation. Il appartient aux services d'exploitation de mener des études de sécurisation spécifiques le cas échéant.

Alinéa d. Gestion des supports et médias informatiques

Les procédures de gestion des supports doivent être établies en fonction de la sensibilité des informations contenues.

Les supports doivent être administrés par une procédure de marquage et de gestion des mouvements tout au long du cycle de vie notamment : lors de l'archivage, de la destruction ou de la diffusion des données. Le chiffrement des données sur leur support est obligatoire pour les informations classifiées «C3» et plus.

Les locaux d'archivage où sont stockés les supports doivent être protégés face aux risques d'accidents (incendie, dégât des eaux, etc.) et d'intrusions.

Le convoyage des supports est soumis à une autorisation du RSSI désigné.

6.4 Sécurité pour les échanges d'informations

Article 1. Principes Généraux

- Les informations doivent être protégées durant leur transmission, en fonction de leur niveau de sécurité.
- Les mesures de sécurité appliquées aux données doivent être recouvrables et réversibles en cas de forces majeures.

Article 2. Les fichiers informatiques

Les fichiers doivent être **chiffrés** si le niveau de classification est **«C3» en confidentialité.**
Les fichiers doivent être **signés** si le niveau de classification est **«C3»ou «C4» en intégrité.**
Les fichiers doivent être **archivés** si le niveau de classification est **«C3»ou «C4» en preuve.**
Les moyens utilisés doivent être validés par le RSSI.

Lors du déploiement de solutions de chiffrement, toutes les précautions devront être prises pour garantir le recouvrement des données chiffrées en cas de perte du mot de passe ou du support qui sert au chiffrement / déchiffrement ou encore lors de départ de personnel.

Article 3. La messagerie électronique

La messagerie électronique peut être employée pour échanger des messages. Cependant, lorsque les informations sont classifiées **au niveau «C3» et plus en confidentialité, l'utilisation d'un moyen de chiffrement est obligatoire.**

Le contenu des messages doit être vérifié en intégrité lorsque le niveau de sensibilité est **classifié «C3»ou «C4» en intégrité : l'utilisation d'une signature est obligatoire.**

6.5 (Télé)maintenance du système d'information

Article 1. Principes Généraux

- Toute maintenance du système d'information doit faire l'objet d'un contrat comportant notamment une clause de confidentialité.
- Les procédures de demande de maintenance, notamment le moyen d'accès aux systèmes informatiques, doivent être définies.
- Toute intervention d'un prestataire externe doit être référencée.

- Une documentation d'exploitation complète par application est tenue à jour systématiquement à chaque modification incluant les consignes de reprises, d'intervention sur incidents et précisant les modes dégradés.

Article 2. Préparation et suivi de l'intervention

Avant l'intervention, les propriétaires des données formalisent leur accord, les mainteneurs sont identifiés et authentifiés, l'intervention est limitée à l'environnement strictement nécessaire.

Pendant l'intervention, le service d'exploitation exerce une surveillance et contrôle l'intégrité de l'environnement. Un journal de toutes les interventions de maintenance logicielle ou matérielle du système d'information doit être tenu à jour. Il indique les modifications effectuées, les solutions apportées et précise l'identité de l'intervenant.

Après l'intervention, le service d'exploitation clôt les moyens d'accès, contrôle l'intégrité de l'environnement et procède le cas échéant aux tests de bon fonctionnement. Un examen des dispositifs de sécurité, voire une reconfiguration des dispositifs, doit être réalisé après chaque intervention de maintenance.

Article 3. Télé-maintenance

Dans le cas de télé maintenance, des moyens spécifiques adaptés aux risques doivent être utilisés (identification/authentification forte, vérification de l'appelant, limitation de la durée de l'intervention, chiffrement des transmissions,…).

Article 4. Maintenance du matériel informatique

Lors d'une intervention de maintenance en atelier, les stations utilisateurs, les serveurs ou les périphériques ne doivent plus contenir d'informations sensibles.

Article 5. Maintenance du matériel réseau et de télécommunication

Lors d'une intervention de maintenance en atelier, les équipements réseaux, les serveurs ou les périphériques ne doivent plus contenir d'informations sensibles.De même, en cas de mise au rebut, les plans d'adressage et autres informations sensibles ne doivent plus être accessibles, présents ou exploitables.

6.6 Mise en place d'une documentation de sécurité

Article 1. Principes Généraux

- Une méthode d'élaboration et de gestion de la documentation de sécurité doit être adoptée.
- La documentation des SI doit faire l'objet de modalités de diffusion spécifiques.
- Le Carnet de Sécurité constitue l'outil de référence en matière de sécurité des systèmes d'information.

Article 2. Règles de gestion documentaire

La sécurité des systèmes d'information est définie par l'ensemble documentaire suivant :

- un Schéma Directeur de Sécurité des Systèmes d'Information ;
- un Cadre Commun de la Sécurité des Systèmes d'Information à partir duquel les politiques de sécurité informatique sont dérivées ;
- un livre blanc pour la protection physique des systèmes d'information ;
- une méthodologie de classification des informations ;
- un guide méthodologique d'application de la classification des informations ;
- un plan type de sécurité des SI par sphère ;
- un tableau de bord de la sécurité type ;
- un registre des PSI publiées.

En fonction du niveau de confidentialité accordé à chaque document, les documents seront disponibles ou non sur un site web intranet de sécurité de l'institution.

Article 3. Règles relatives au Carnet de Sécurité des Systèmes d'Information

Ce carnet a vocation à être renseigné tout au long du cycle de vie du système d'information par l'ensemble des acteurs impliqués dans les processus de conception, de développement et d'exploitation des systèmes d'information.
Chaque dossier de sécurité produit au cours du cycle de vie du système d'information se doit d'être intégré dans le carnet de sécurité lequel sera partagé par tous les acteurs impliqués.

Le carnet de sécurité contient :

- le dossier d'expression de besoins émanant de la maîtrise d'ouvrage ;
- les exigences de sécurité requises ;
- le cahier de spécifications fonctionnelles précisant :
  - le choix des fonctions et des mécanismes de sécurité
  - la définition des tests de sécurité
- le cahier de spécifications techniques précisant :
  - l'architecture technique retenue
  - les règles de codification des éléments de sécurité
  - le cahier de qualification de la sécurité
  - le dossier CNIL
- le cahier d'exploitation spécifiant :
  - les consignes d'installation
  - les consignes d'utilisation
- les modalités de fin de vie du système d'information.

La complétude du carnet de sécurité relève de la responsabilité du chef de projet garant de la bonne application des procédures.
Le carnet de sécurité fait l'objet d'une validation par les instances de pilotage et les RSSI.

Le carnet de sécurité doit être tenu à jour tout au long du cycle de vie du système. En fonction de l'âge du système certaines pièces du carnet de sécurité peuvent nécessiter d'être archivées.

6.7 Limitation des sinistres du système d'information

Article 1. Principes Généraux

- Un plan de reprise d'activité du système d'information doit être formalisé et testé.
- Un réseau d'alerte doit être mis en place pour traiter les incidents de sécurité et appliquer les procédures adéquates.
- Les incidents de sécurité doivent être catégorisés et traités pour éviter la compromission d'informations sensibles.
- Les incidents de sécurité doivent être analysés et documentés afin de capitaliser l'expérience.
- Une évaluation du niveau de confiance accordé au système d'information peut être effectuée.

Alinéa a. Plans de sauvegarde

Le plan de sauvegarde est établi et maintenu par le service d'exploitation. Des tests de restauration sont réalisés périodiquement.
Le mode de sauvegarde des données des systèmes d'information doit garantir un niveau de sécurité suffisant pour une exploitation ultérieure.
La durée de conservation des sauvegardes doit être définie, en fonction de la sensibilité du site, de la zone et des usagers concernés et du cahier des charges fonctionnels.
La fréquence, la duplication et les lieux de sauvegarde sont fonction de la politique de sécurité du site.
Un contrôle des supports, de l'appareillage de sauvegarde ainsi des tests de restauration doivent être réalisés régulièrement.
Les copies de sauvegardes sont systématiquement conservées dans un local protégé des risques accidentels et d'intrusions.
Tout usager doit pouvoir disposer d'un espace de stockage pour sauvegarder ses données professionnelles.

Un plan de reprise d'activité du système d'information doit être formalisé et testé.

Plan de sauvegardes des logiciels de production

L'ensemble des configurations doit être systématiquement sauvegardé à la fois sur le site de production et à l'extérieur. Chaque site de production doit disposer d'une procédure permettant, à tout moment, de reconstituer à partir des sauvegardes l'environnement de production.

Plan de sauvegardes des données applicatives

Le plan de sauvegarde des données applicatives doit faire l'objet d'une étude afin :

- d'identifier les scénarii de risques pour lesquels les sauvegardes de données applicatives doivent être restaurées ;
- de déterminer la fréquence de sauvegardes compatibles avec les exigences de la maîtrise d'ouvrage.

Une procédure doit contrôler que le redémarrage de l'activité est effectivement possible à partir des sauvegardes réalisées.

Alinéa b. Plan de secours

Un plan de secours a pour objectif d'assurer le maintien d'une activité critique.
Il se compose de deux volets :

- volet conceptuel : établi par le chef de projet en réponse aux besoins exprimés par la maîtrise d'ouvrage en coordination avec les responsables administratifs et / ou gestionnaires du domaine d'activités couvert par le SI ;
- volet opérationnel : établi par le service d'exploitation et validé par le RSSI.

Par ailleurs, il appartient au RSSI de contrôler la mise à jour du plan de secours et de le diffuser. Chaque scénario de risque majeur identifié est décomposé de la manière suivante :

- Comment et par qui la crise peut être détectée ?
- Quelles sont les actions à entreprendre lors de la survenance de l'incident?
- Quelle est la chaîne d'alerte à activer?

Le plan de secours

- décrit les responsabilités et les opérations qui doivent être menées pour assurer la continuité des services et garantir le fonctionnement des ressources critiques jusqu'au retour normal des conditions d'exploitation ;
- définit les procédures d'escalade à appliquer et la nature des alertes à remonter ;
- mesure les impacts probables d'un sinistre et décrit les modalités de restauration en cas d'une altération de données ;
- prévoit une solution alternative de remplacement pour tous les composants (matériels ou logiciels) endommagés demandant une forte disponibilité ;
- prévoit des délais maximum d'interventions compatibles avec les exigences de disponibilité définies par la maîtrise d'ouvrage ;
- prévoit les mesures spécifiques à appliquer lorsque le temps de l'intervention dépasse la durée fixée par les parties.

Les solutions de secours doivent être parfaitement opérationnelles et dimensionnées pour absorber une charge minimale suffisante définie par la maîtrise d'ouvrage.

Le plan de reprise décrit en détail

- les solutions de secours ;
- les règles de déclenchement ;
- les actions à mener ;
- les priorités de reprise ;
- les acteurs à mobiliser et leurs coordonnées.

La défaillance ou l'indisponibilité des moyens de secours doivent également être envisagées pour les équipements très critiques.

Article 2. Tableaux de bords et Pilotage de la Sécurité

L'évaluation du niveau de confiance accordé au système d'information repose sur l'élaboration d'un tableau de bord qui permet de faire une vérification périodique du niveau de couverture des risques à travers des indicateurs de vulnérabilité, de risques et d'incidents. On distingue deux catégories d'incidents : les incidents majeurs et les incidents

courants. Il est nécessaire de définir les seuils de gravité pour déterminer les incidents qui doivent être considérés comme majeurs.

Typologie d'incident	Gravité
Evènement naturel ou accident (incendie, dégâts des eaux, …)	Majeur dès que l'évènement provoque une indisponibilité du système d'information bloquante pour les «utilisateurs»
Erreur de manipulation, de programme, …	Majeur dès que la réparation nécessite une charge supérieure à 1 homme / mois
Malveillance (altération volontaire ou vol de données, intrusion, divulgation, …)	Majeur dans tous les cas
Virus	Majeur dès que la réparation nécessite une charge supérieure à 1 homme/mois
Interruption de service (panne de matériel, saturation de serveurs ou du réseau, …)	Majeur dès que l'évènement provoque une indisponibilité du système d'information bloquante pour les «utilisateurs»

Les responsables de domaine doivent prendre les mesures nécessaires pour détecter un incident majeur et effectuer les investigations a posteriori.

Les traces peuvent servir de preuves et doivent être conservées. En fonction de la politique de sauvegarde, un archivage peut être nécessaire pour couvrir la période de conservation.

Toute personne constatant un incident majeur est tenue d'alerter dans les délais les plus brefs son RSSI qui diffuse l'alerte. Les procédures de réaction aux incidents servent à faire connaître le plus rapidement possible et le plus fidèlement possible un incident à la collectivité.

Les incidents sont consignés dans un manuel d'exploitation.

Pour chaque incident, le RSSI met à jour une base de données des incidents majeurs et courants qui comprend :

- la description de l'évènement ;
- les circonstances de l'évènement ;
- les causes identifiées ou possibles ;
- les conséquences sur les personnes, les équipements et les informations ;
- les décisions et les mesures prises.

Les incidents sont suivis par des indicateurs définis soit par le contrat de service d'exploitation, soit par le service d'exploitation lui-même. Les indicateurs sont consolidés dans des tableaux de bord mentionnant des évènements tels que le nombre d'incidents réels détectés, la disponibilité des applications, le nombre de badges d'accès perdus, les pannes des composants de sécurité, etc.
Une synthèse des incidents est incluse dans le tableau de bord de la sécurité.

Dans le cadre de leur mission de contrôle, le RSSI doit effectuer (lui- même ou en s'appuyant sur des partenaires spécialisés) des vérifications :

- conformité technique : la mise en œuvre correcte des mesures de sécurité concernant les matériels ou les logiciels ;
- des tests d'intrusion ;
- des tests de comportement des «utilisateurs».

6.8 Application des ITSEC pour une évaluation de la sécurité du système d'information

Voir aussi : **chapitre 6 – 6.1 - (Article 5.** Cadre méthodologique «Sécurité et Développement»)

Pour respecter la réglementation , une évaluation du niveau de confiance accordé au système d'information pourra être effectué.

6.9 Anticipation pour l'évolution de la sécurité du système d'information

Une veille technologique active doit être mise en place afin de garder un niveau de sécurité du système d'information conforme à cette politique générale.