Schéma directeur de la sécurité des systèmes d'information
organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives

Schéma directeur de la sécurité des systèmes d'information
organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives

ministère de l'Éducation nationale,
de l'Enseignement supérieur
et de la Recherche
mars 2005

Préface

Les technologies de l'information et de la communication, leurs usages pédagogiques et professionnels connaissent une montée en puissance. Les espaces numériques de travail dédiés aux élèves, aux étudiants, aux personnels se multiplient. L'administration électronique se développe rapidement. Dans cette perspective, il importe de mettre en œuvre les conditions d'une confiance accrue dans l'esprit d'une démarche qualité. La sécurité des systèmes : un problème essentiel, majeur ; leur complexité les rend vulnérables car elle accroît les failles non repérées par les concepteurs.

Les systèmes d'information s'ouvrant de plus en plus vers l'extérieur, ils doivent le faire dans un cadre sécurisé et maîtrisé. Dans ce domaine, le service public d'éducation doit se montrer exemplaire.

Avec la modernisation de l'administration et l'évolution des réglementations publiques nationales et européennes, ce schéma directeur de la sécurité des systèmes d'information se révèle un outil indispensable et essentiel, adapté au contexte, pour garantir et coordonner toute la sécurité attendue dans la généralisation de leurs usages par les communautés éducatives.

Des règles éthiques et déontologiques sont par exemple nécessaires en ce qui concerne les usages des TIC par les élèves et personnels de l'Éducation nationale.

Cette politique de sécurité doit être communiquée et expliquée pour responsabiliser les utilisateurs. Une chaîne de responsabilité et d'alerte est mise en place.

Depuis avril 2002, les différents acteurs de l'Éducation nationale, au plan pédagogique et administratif, s'associent largement, dans les académies, aux travaux réalisés par la Direction des Personnels, de la Modernisation et de l'Administration en liaison avec plusieurs partenaires. Cette réflexion a abouti à l'élaboration et la mise en œuvre d'un plan d'action sécurité des systèmes d'information sur trois années, de 2004 à 2007.

Je souhaite à toutes et à tous un bon usage de ces nouveaux outils qui permettent de façon créative et sûre de faire évoluer notre administration et notre enseignement vers plus de souplesse en répondant de façon plus individualisée aux attentes des personnels et des usagers tout en préservant la sécurité de l'ensemble des données. Ce schéma directeur devrait aider à réussir le pari de la sécurité des TIC de façon globale, efficace et solidaire.

Dominique Antoine
Directeur des Personnels,
de la Modernisation et de l'Administration

Message de Bernard Vors, Haut Fonctionnaire de Défense

L'accroissement des risques de toute nature auxquels sont soumis les systèmes d'information a conduit le Premier ministre à demander en avril 2003 d'établir un plan de renforcement de la sécurité des systèmes d'information de l'État (PRSSI). Ce plan, consultable à l'adresse http://www.ssi.gouv.fr/fr/documentation/PRSSI, doit couvrir les moyens de communication et les systèmes d'information, en termes de capacités opérationnelles de réponse aux attaques informatiques et de gestion de crise. Cette stratégie française en matière de défense et de sécurité est à considérer dans une perspective européenne.
Pour atteindre les objectifs visés, le plan comporte des mesures concernant la formation et les compétences, l'organisation, les équipements, le tissu industriel et le cadre juridique. La mise en œuvre du PRSSI doit être menée sur la période 2004 à 2007 tant au niveau interministériel qu'au niveau de chaque département ministériel.

Le premier domaine évoqué, celui de la formation et des compétences, est au cœur de métier de notre ministère. Il s'agit donc de promouvoir le thème de la SSI au niveau des formations scolaires et supérieures, ainsi que de renforcer les formations des maîtres et la formation continue, tout en tirant le meilleur parti possible de l'enseignement en ligne. D'ores et déjà, une convention se met en place entre le SGDN, le MENESR et le CNED.

Le domaine organisationnel s'inscrit dans ma mission ministérielle relative à la sécurité des systèmes d'information en tant que haut fonctionnaire de défense, conformément au décret consultable à l'adresse http://www.legifrance.gouv.fr/texteconsolide/PHHYT.htm. Au titre des mesures organisationnelles, le PRSSI prévoit explicitement l'élaboration d'un schéma directeur de la SSI, ainsi que la mise en place d'une chaîne fonctionnelle de la SSI. Le schéma directeur est au stade de la publication aujourd'hui et je tiens à saluer le travail de toutes les personnes ayant participé à ce projet tant au niveau du pilotage que des groupes de travail,

des comités de lecture, des animations et des communications. Ce projet d'envergure, initié d'ailleurs avant la demande du Premier ministre de 2003, vient donc à point nommé.

Il reste à officialiser et renforcer la chaîne fonctionnelle en matière de SSI qui formalisera en fait le rôle des acteurs de la mise en œuvre et du suivi du schéma directeur. Cette chaîne doit s'inspirer de la recommandation interministérielle n°901/DISSI/SCSSI du 2 mars 1994 disponible à l'adresse http://www.ssi.gouv.fr/fr/reglementation/901. Cette recommandation est relative à la protection des systèmes d'information traitant des "informations sensibles non classifiées de défense". Elle définit les grandes orientations de la politique à mettre en œuvre par les départements ministériels pour assurer la protection des informations dans le respect des lois et règlements en vigueur. Elle précise également l'organisation à mettre en place pour appliquer cette politique. Elle définit et répartit les responsabilités entre les différents intervenants dans ce domaine.

En point d'entrée de la chaîne fonctionnelle, on trouve au niveau de chaque ministère le haut fonctionnaire de défense (HFD) et le fonctionnaire de sécurité des systèmes d'information (FSSI). Notre Ministre a nommé en juillet dernier un FSSI en la personne de Mme Isabelle Morel, ce qui a été d'ailleurs une première pour notre ministère qui ne disposait pas d'un FSSI auparavant. La chaîne se prolonge ensuite pour chaque grande entité du ministère par une "autorité qualifiée pour la sécurité des systèmes d'information" (AQSSI) et un "responsable de la sécurité des systèmes d'information" (RSSI).

Comment appliquer cette recommandation à notre communauté "éducation, enseignement supérieur et recherche" ? Certes, les métiers sont différents mais un certain nombre de préoccupations sont néanmoins communes. En outre, c'est une communauté d'utilisateurs fortement interconnectés. Cette interconnexion fait que la robustesse aux attaques se mesure au maillon le plus faible et en fait une communauté interdépendante. La manifestation physique de cette interdépendance se

voit bien au travers des réseaux RENATER et RACINE qui illustrent bien la mutualisation et l'interdépendance de cette communauté.

En conséquence, notre organisation en matière de SSI doit s'appliquer à un vaste périmètre correspondant à l'administration centrale, l'administration déconcentrée (rectorats et EPLE), aux établissements publics sous tutelle du ministère, aux universités et aux autres organismes publics dépendant ou sous tutelle du ministère – IUFM, écoles d'ingénieurs, groupements d'intérêts publics, etc.

Conformément à la recommandation, chacune de ces entités devra voir la responsabilité de la SSI confiée à l'autorité qualifiée (AQSSI) qui n'est autre que le responsable juridique concerné, notamment : recteur, président, directeur général. Cette notion d'"autorité qualifiée" recouvre l'exercice de la maîtrise d'ouvrage, la responsabilité de passer les actes contractuels mais aussi la responsabilité de mettre en place des organisations, de faire des arbitrages budgétaires en terme d'équipements, de services et de moyens humains, la responsabilité d'intenter des actions en justice…

L'AQSSI est assisté par un RSSI qu'il nomme et mandate pour mettre en place et veiller à la bonne réalisation de la politique générale de sécurité qu'il a lui-même impulsée. Des RSSI sont nommés progressivement dans toutes les entités du ministère, au sens du périmètre évoqué plus haut. Leur travail est remarquable et je pense qu'ils méritent une meilleure reconnaissance. C'est cette position de rattachement direct auprès de l'AQSSI qui leur conférera toute leur légitimité et qui leur permettra d'assurer pleinement leur mission.

Je voudrais en dernier lieu rappeler le domaine que nous avons à protéger. Les menaces peuvent prendre des formes plus ou moins aiguës et mener à des situations de crises relativement importantes. Chacun de nous connaît l'état de crise permanente qui est devenue malheureusement un peu la vie de tous les jours, résultat d'attaques de virus presque routinières. Et puis il y a des crises plus aiguës, relativement fréquentes, résultat de virus plus

offensifs qui désorganisent quelques jours l'administration des systèmes et qui dans certains cas détériorent la qualité et la fiabilité des informations partagées. Enfin, il y a la crise majeure, à caractère exceptionnel, à laquelle il faut se préparer. En pratique, cela signifie le besoin de décliner au niveau de chaque entité du ministère, ce qu'on appelle le plan de prévention Vigipirate dans sa composante informatique et le plan de crise Piranet. Il s'agit là aussi d'une mission spécifiquement dévolue aux AQSSI et à leur RSSI. C'est un de nos grands chantiers à mener. Il s'inscrit dans le volet d'actions "mise en place et animation de la chaîne de responsabilité et d'alerte" du SDSSI.

Bernard Vors
Haut Fonctionnaire de Défense

Sommaire

1. Introduction

1.1 Préambule

Le Schéma Directeur de Sécurité Systèmes d'Information (SDS SI) est un projet prioritaire s'inscrivant dans un cadre de modernisation des systèmes d'information, de personnalisation des accès et d'ouverture à tous de l'usage des technologies de l'information et la communication (TIC) avec le niveau de sécurité attendu.

Le Schéma Directeur de Sécurité s'inscrit dans une démarche méthodologique consistant à ouvrir tous les trois ans un grand chantier dans le domaine de la sécurité des systèmes d'information (SSI) dans l'optique :

- **de vérifier que l'organisation mise en œuvre est opérationnelle et performante ;**
- **d'actualiser les axes d'orientation au regard des évolutions technologiques ;**
- **de mesurer l'adéquation entre les enjeux de la SSI et les risques encourus ;**
- **d'évaluer la compatibilité des moyens accordés avec les objectifs visés ;**
- **d'actualiser le plan d'action SSI.**

1.2 Objet du document

Le Schéma Directeur de la Sécurité des Systèmes d'Information vise à :

- **expliciter les contextes de mise en œuvre du schéma directeur ;**
- **identifier et préciser les enjeux de la sécurité pour les communautés éducatives ;**
- **définir une organisation et préciser les responsabilités à tous les échelons de l'Éducation nationale ;**

- **offrir un cadre commun pour la définition et la mise d'œuvre des politiques de sécurité dédiées ;**
- **fixer les orientations techniques sous-jacentes aux projets de modernisation des systèmes d'information (SI) ainsi qu'au développement sécurisé de l'administration électronique ;**
- **et enfin, à traduire les objectifs de sécurité sous forme de plans d'actions opérationnels.**

1.3 Cadre d'élaboration du schéma directeur de la sécurité des systèmes d'information

1.3.1 Contexte politique et stratégique

L'élaboration d'une **politique de sécurité des systèmes d'information** (PSSI) revêt un **caractère stratégique** pour le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.

Cette politique s'inspire de l'effet conjugué, d'une part, de la généralisation de l'utilisation des technologies de l'information et, d'autre part, des menaces spécifiques que ces technologies induisent en terme de fonctionnement.

De ce fait, l'institution est amenée à :
- **déterminer la politique de sécurité des systèmes d'information** (arbitrages entre sécurisation et ouverture absolue des services par exemple) ;
- **renforcer ses capacités de protection des systèmes d'information** dans le cadre du PRSSI interministériel (Plan de Renforcement de la Sécurité des Systèmes d'information) ;
- **mobiliser des moyens dédiés et à procéder aux nécessaires** mutualisations des ressources et compétences.

Par ailleurs, la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) du Secrétariat Général de la Défense

Nationale (SGDN) incite chaque département ministériel à mettre en œuvre la recommandation interministérielle relative à la protection des systèmes d'information traitant des information sensibles non classifiées de défense (n° 901du 2 mars 1994).

Cette recommandation définit les grandes orientations de la politique de sécurité à mettre en œuvre en matière de sécurité des systèmes d'information, pour assurer la protection des informations sensibles non classifiées de défense, dans le respect des lois et règlements en vigueur. Elle précise également l'organisation à mettre en place pour appliquer cette politique. Enfin, elle définit et répartit les responsabilités entre les différents intervenants dans ce domaine.

1.3.2 Contexte juridique

Le schéma directeur de la sécurité des systèmes d'information découle également d'une prise **en compte au plus haut niveau de l'institution de l'évolution des réglementations publiques nationales et européennes.**

Ainsi, la loi a progressivement pris en compte l'importance des TIC, prévoyant dès 1978 de protéger la vie privée des personnes (loi «informatique et libertés») jusqu'à encadrer l'économie numérique en 2004.

La réglementation en vigueur engage la responsabilité de personnes physiques et morales autant dans le système éducatif que dans l'ensemble de la société d'où la nécessité d'organiser la sécurité des systèmes d'information.

1.3.3 Contexte institutionnel et organisationnel

La place de plus en plus importante des collectivités régionales, départementales et locales dans le fonctionnement matériel des établissements et des écoles, leur implication progressive dans la

mise à disposition de ressources numériques à travers les espaces numériques de travail (ENT), leur importance croissante autour de la vie scolaire, les relations des établissements et écoles avec leur environnement, rendent indispensable leur participation à l'élaboration et à la mise en œuvre des plans de sécurité des systèmes d'information (P2SI) des établissements et écoles, ainsi que l'adaptation des dispositions aux spécificités locales, départementales et régionales.

Au sein du système éducatif, élèves, étudiants, enseignants, enseignants-chercheurs et personnels administratifs se partagent tous l'usage des systèmes d'information. Le niveau d'appréhension, la perception des objectifs et des contraintes peuvent sembler différents selon le type d'acteur concerné.

C'est pourquoi la sécurité des systèmes d'information, particulièrement dans le monde de l'éducation, doit tenir compte de la diversité des acteurs, du partage des responsabilités défini dans le cadre de la loi, de la spécificité des communautés territoriales et des communautés éducatives.

Cependant cette diversité ne doit pas être un frein à la formation et la sensibilisation de l'ensemble des usagers du ministère.

1.3.4 Contexte technique

L'évolution des moyens techniques est à l'origine d'une interaction forte entre systèmes d'information, systèmes informatiques et organisations. Aujourd'hui, l'importance accrue des réseaux du fait d'un déploiement massif des postes de travail informatiques **rend leur fiabilité et leur disponibilité impérative.**

L'accroissement des performances des matériels, combinée aux fortes baisses de coûts, a progressivement amené les systèmes d'information à se substituer aux modes de travail traditionnels vers

lesquels il ne saurait être envisageable de revenir, ne serait-ce que ponctuellement.

Cette nouvelle organisation tend à abolir la notion d'espace de travail géographiquement localisé, mais cette souplesse absolue nécessite d'imposer des mesures strictes de cloisonnement des réseaux comme de règles de confinement des zones d'interopérabilité.

La sécurité des systèmes d'information doit s'inscrire dans un cadre technique maîtrisé.

1.4 Enjeux de sécurité des systèmes d'information

L'enjeu majeur est d'offrir un service public d'enseignement basé sur des systèmes d'information fiables disposant d'un niveau de sécurité adéquat et de fournir ainsi un cadre protecteur pour l'utilisation des technologies de l'information et de la communication.

Comme dans la plupart des grandes organisations, les systèmes d'information de l'Éducation nationale peuvent être pris pour cible et de ce fait, conduire à un déni de service : ils ne font pas exception.

Des facteurs internes ou externes (vulnérabilités intrinsèques aux matériels, logiciels, réseaux, organisations, locaux et personnels) peuvent renforcer la fragilité des systèmes ou l'appétence de pirates informatiques. La complexité des organisations, la multiplicité d'éléments «stratégiques» pour le fonctionnement général des SI, le fait que l'école se retrouve régulièrement au cœur du débat sociétal en cristallisant les attentions, sont autant de facteurs à maîtriser.

Dans le cadre d'une Stratégie Ministérielle de Réforme (SMR), le ministère de l'Éducation nationale dans sa globalité poursuit le développement d'une administration électronique s'ouvrant plus encore aux citoyens, en prenant en compte la pluralité des lieux

d'accès à l'information : de l'établissement scolaire au domicile de l'élève, de l'université au domicile de l'étudiant ou des services de gestion au domicile de l'agent.

Dans cette logique d'ouverture, le respect de la liberté individuelle de tout acteur ou usager du système éducatif doit demeurer une préoccupation constante. La maîtrise de la sécurité des systèmes d'information accompagne le développement des espaces numériques de travail (ENT) dédiés aux élèves, étudiants et enseignants. Elle doit également garantir la disponibilité des services au cœur des systèmes d'information et offrir un socle de données fiables et intègres.

Dans un système éducatif en prise directe avec la société civile, la sécurité informatique ne doit pas s'imposer comme une contrainte inéluctable mais s'inscrire dans une démarche «qualité» en recherchant l'adhésion des usagers. C'est pourquoi une politique de sécurité des systèmes d'information doit être élaborée en respect du contexte et communiquée avec suffisamment d'explications pour responsabiliser et faire adhérer les utilisateurs. Il est important de conserver à l'esprit que la SSI repose bien souvent in fine sur l'utilisateur.

Nota : par convention dans la suite du document, par «ministère», nous entendons le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.

2. Orientations de la sécurité dans le système éducatif

Le système éducatif, riche de par la diversité de ses utilisateurs et de ses établissements, doit répondre à des besoins de sécurité de ses systèmes d'information. Conscient de la multitude d'établissements ayant parfois des problématiques de sécurisation

des systèmes très différenciés, l'institution est convaincue de la nécessité d'aborder ce sujet dans le cadre d'une organisation systémique et globale.

Le Système d'Information doit être appréhendé dans son ensemble avec une analyse croisée des enjeux application par application, entité par entité, service par service. Une attention particulière doit être portée à la mise en cohérence des politiques de sécurité pour éviter d'élaborer des mesures différentes traitant des niveaux de sécurité identiques ou inversement.

Ceci implique naturellement une juste appréciation des risques et des enjeux par les **maîtrises d'ouvrage, responsables de domaines fonctionnels** et la nécessaire mobilisation des acteurs exploitant les ressources informatiques de l'institution (serveurs, réseaux, postes de travail ouverts sur l'intranet et l'Internet…).

La prise en compte de la sécurité doit également s'apprécier tout au long du cycle de vie des systèmes d'information. Ainsi, tout projet devra intégrer un volet sécurité pour chacune des phases de conception, réalisation, tests de validation, homologation, mise en production, maintenance et fin de vie.

Tout projet doit disposer d'un carnet de sécurité ouvert aux acteurs concernés et dans lequel tout élément relatif à la sécurité y est consigné (cf supra § 2.1.2).

Plus généralement, **tous les acteurs du système éducatif** sont concernés par la sécurité du système d'information éducatif.

À ce titre, l'institution met à la disposition de tous, chacun à son niveau, l'information et les outils méthodologiques et techniques appropriés.

La sécurité des systèmes d'information devra prendre en compte **les éléments fondamentaux suivants :**

- **L'identification sans ambiguïté des différents acteurs de la sécurité**

des systèmes d'information au sein d'une chaîne fonctionnelle SSI connue et reconnue.

- **La prise en compte de la sécurité dans tout projet «systèmes d'information».**
- **La prise de compte des diverses catégories d'usagers de la communauté éducative.**
- **L'utilisation des chartes nationales (validées par la CNIL) relatives aux usages et aux utilisateurs des systèmes d'information du ministère de l'Éducation nationale.**
- **La mise en œuvre d'une politique de sécurité des systèmes d'information pour le ministère.**

2.1 Sécurité et conception des systèmes d'information

La problématique de la sécurité des systèmes d'information doit être prise en compte le plus en amont possible d'un projet, à savoir, dès sa conception. Elle se doit également d'en couvrir tous les volets, du développement à la mise en exploitation sur les réseaux en passant par les systèmes.

Il s'agit donc, pour chaque projet, de bien spécifier les besoins de sécurité afin d'être capable d'en **mesurer les impacts sur la continuité de l'activité.**

L'objectif ici recherché sera bien de répondre aux interrogations suivantes :

- Quels risques encourt le système d'information mis en place ?
- Quels objectifs de sécurité doivent être satisfaits et quels niveaux de sécurité appliqués?
- Quelles solutions peuvent être mises en place ?
- Quels sont les risques non couverts ?

La mise en œuvre de la démarche est primordiale mais nécessite néanmoins de clarifier au préalable, d'une part, les rôles respectifs

des maîtrises d'ouvrage et maîtrises d'œuvre dans le processus de prise en compte de la sécurité des systèmes d'information, et d'autre part, de formaliser ou d'adopter des outils méthodologiques de suivi et de consignation des éléments de sécurité.

2.1.1 Rôles des maîtrises d'ouvrage et des maîtrises d'œuvre

a. Rôles des maîtrises d'ouvrage

Le rôle de la maîtrise d'ouvrage (MOA) doit être **prépondérant** dans la définition des enjeux de sécurité liés aux systèmes d'information. Le maître d'ouvrage devra ainsi identifier les éléments essentiels devant être protégés (il s'agit du patrimoine informationnel vital pour l'institution et ses établissements associés : informations et fonctions).

Le maître d'ouvrage devra également organiser l'expression des besoins de sécurité des éléments essentiels selon une classification donnée en termes de disponibilité, d'intégrité, de confidentialité (confidentielles ou non classifiée par exemple)…

Le maître d'ouvrage se chargera de lister les **profils d'usagers** ayant accès aux informations classifiées et déterminera les **fonctionnalités autorisées.**

Le maître d'ouvrage devra organiser une étude des menaces pesant sur les SI. Il s'agira d'étudier les méthodes d'attaques qui peuvent être employées par des éléments menaçants, en exploitant des vulnérabilités du SI.

Le maître d'ouvrage doit être en mesure d'exprimer ses objectifs de sécurité, au même titre que les besoins fonctionnels.

Une méthodologie d'expression des besoins et d'identification des objectifs de sécurité basée sur les recommandations de la **Direction Centrale de Sécurité des Systèmes d'Information** (DCSSI)

est mise à disposition des maîtrises d'ouvrage : celles-ci pourront faire appel le cas échéant à des prestations d'assistance à **maîtrise d'ouvrage**. La méthode préconisée est annexée au SDS SI.

Les éléments méthodologiques d'expression des besoins propres au ministère de l'Éducation nationale sont référencés et annexés dans le présent document.

b. Rôles des maîtrises d'oeuvre

La maîtrise d'œuvre (MOE), sous la responsabilité **du chef de projet et de l'architecte des systèmes d'information**, prend en compte les objectifs de sécurité exprimés par la maîtrise d'ouvrage dans la phase amont de conception d'un SI.

Le chef de projet

Le chef de projet analyse les objectifs de sécurité identifiés par la MOA pour proposer des solutions (sous la forme d'exigences de sécurité).

Il vérifie notamment que les solutions retenues sont bien en adéquation avec les objectifs de sécurité identifiés par la maîtrise d'ouvrage. Il intègre la problématique SSI dans le projet en se faisant assister d'un expert SSI en tant que de besoin.

L'architecte des systèmes d'information

L'architecte **définit et formalise**, en liaison avec le chef de projet, les mesures de sécurité externes au système d'information mais nécessaires à la mise en œuvre du niveau de sécurité requis (authentification forte, passerelles de sécurité, cloisonnement de réseaux etc.).

La maîtrise d'œuvre **évalue les risques non couverts** par le dispositif de sécurité et **les fait valider par la maîtrise d'ouvrage.**
La maîtrise d'œuvre **assiste** également la maîtrise d'ouvrage dans la rédaction du dossier de la CNIL (Commission Nationale Informatique et Libertés).

2.1.2 Le carnet de sécurité du système d'information

Toute application ou système d'information doit disposer d'un carnet de sécurité. Ce carnet constitue l'outil de référence en matière de SSI.

Ce carnet a vocation à être renseigné tout au long du cycle de vie du SI par l'ensemble des acteurs impliqués dans le processus de développement et de l'exploitation des SI.

Chaque dossier de sécurité produit au cours du cycle de vie du SI 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'identification des objectifs de sécurité émanant de la MOA.
- Les exigences de sécurité déterminées par la MOE.
- Le cahier de spécifications fonctionnelles précisant :
  - le choix des fonctions et des mécanismes de sécurité choisi pour couvrir les exigences 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 cas échéant).
- Le cahier d'exploitation spécifiant :
  - les consignes d'installation
  - les consignes d'utilisation.

La complétude du carnet de sécurité relève de la responsabilité du chef de projet garant de la bonne application des procédures.
La mise en production d'un SI est conditionnée par le respect des règles consignées dans le carnet de sécurité mais également par la prise en compte de la PSSI du site hébergeur.

Des procédures de contrôle permettent de vérifier la continuité et la qualité du service offert aux utilisateurs et services. Ces procédures sont décrites dans le plan de sécurité des systèmes d'information (P2SI supra 2.4) de l'entité concernée.

Le carnet de sécurité est matérialisé par une application collaborative gérée et hébergée par un pôle d'expertise spécialisé.

2.2 Acteurs de la sécurité opérationnelle des systèmes d'information

En préalable à l'identification des acteurs de la sécurité des systèmes d'information, il convient de rappeler le constat suivant : **les défaillances de sécurité trouvent leur cause, dans leur grande majorité, dans des comportements humains inappropriés.**

En conséquence, les **utilisateurs internes** des systèmes d'information du ministère doivent **être informés de leur responsabilité individuelle** en matière de sécurité des systèmes d'information dans le cadre de leur fonctions ou des missions qu'ils exercent au sein de l'institution.

Ceci implique également que chacun puisse **disposer des éléments d'informations organisationnels** nécessaires pour faire face à des situations d'attaques logiques ou des perturbations du fonctionnement de leur environnement de travail.

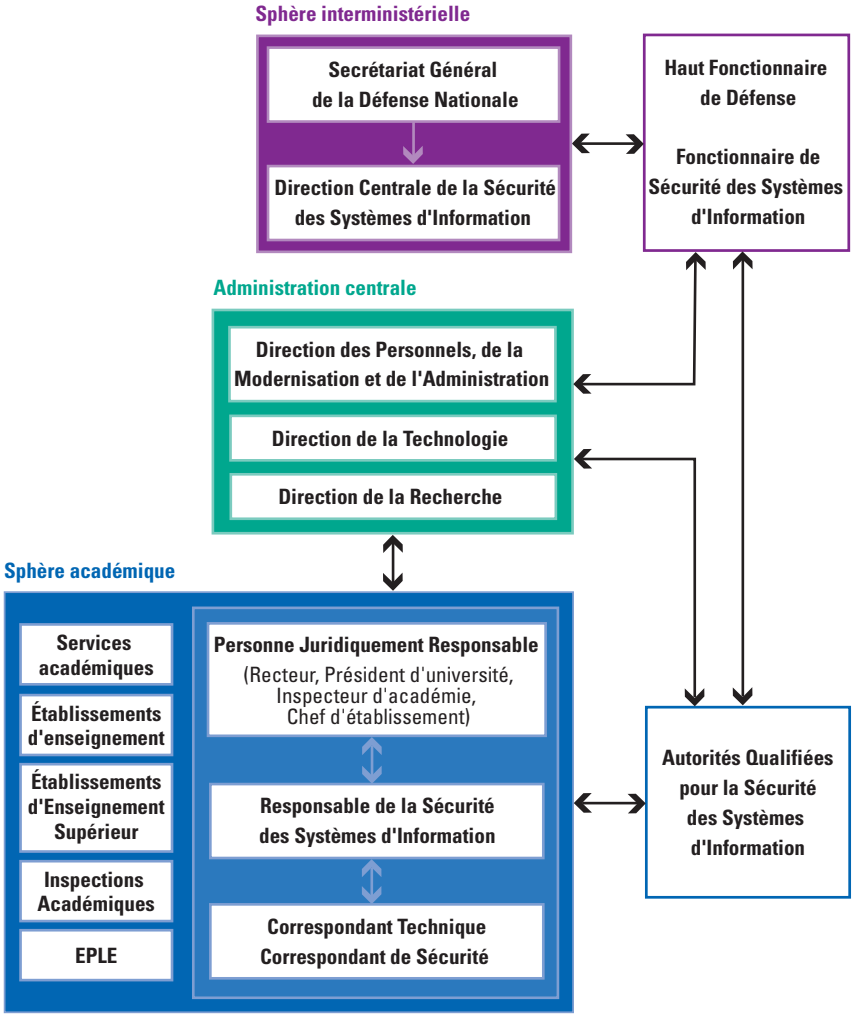
En effet, en dépit de la complexité des technologies déployées pour prévenir les risques ou protéger les systèmes d'information, il convient **de réaffirmer la prééminence du facteur humain dans l'organisation de la sécurité des systèmes d'information (SSI).**

Il s'agit donc bien, dans un premier temps, de recenser les acteurs concernés ou impliqués à quelque titre que ce soit par cette problématique globale de sécurité.

Interviennent dans le domaine de la SSI :

- Le haut fonctionnaire de défense et ses services.
- Les directions «opérationnelles».
- Les autorités hiérarchiques.
- Les responsables de la sécurité des systèmes d'information.
- Les correspondants techniques de sécurité.

La chaîne d'alerte et de responsabilité s'organise comme suit :



2.2.1 Le service du Haut Fonctionnaire de Défense

La sécurité des systèmes d'information relève de la responsabilité de chaque ministre, pour le département dont il a la charge.

Il est assisté par un Haut Fonctionnaire de Défense (HFD), responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information.

Un Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) est désigné par le ministre et placé sous l'autorité du Haut Fonctionnaire de Défense.

Ses fonctions sont définies dans la recommandation interministérielle n° 901 référencée au §1.3.1.

Le ministre désigne des Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI) dans les administrations centrales, les services déconcentrés de l'Etat, organismes et établissements publics relevant de sa tutelle.

Sous le contrôle du HFD et du FSSI l'autorité qualifiée est chargée des missions définies dans la recommandation interministérielle n° 901 référencée au §1.3.1.

Les AQSSI sont assistés d'Agents de Sécurité des Systèmes d'Information (ASSI) dans la gestion et le suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent leurs responsabilités.

2.2.2 Les directions opérationnelles

Les trois directions opérationnelles, dans le pilotage de la mise en œuvre de la Sécurité des Systèmes d'information à l'aide du Haut Fonctionnaire de Défense, sont identifiées ci-dessous :

- Direction des Personnels, de la Modernisation et de l'Administration (DPMA).
- Direction de la Technologie (DT).
- Direction de la Recherche (DR).

a. Direction des Personnels, de la Modernisation et de l'Administration

La DPMA met en œuvre la sécurité des systèmes d'information dans les services académiques et les établissements scolaires.

b. Direction de la Technologie

La Direction de la Technologie est maître d'ouvrage dans le domaine du développement des usages pédagogiques des TIC.

C. Direction de la Recherche

La Direction de la Recherche, s'appuyant sur le Comité Réseau des Universités (CRU) ainsi que sur les instances de la Conférence des Présidents d''Universités (CPU), coordonne la mise en œuvre de la sécurité des systèmes d'information adaptée à l'enseignement supérieur et la recherche.

2.2.3 L'autorité hiérarchique ou «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 l'application de la PSSI.

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 d'une

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 (PSSI) 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 (RSSI).

2.2.4 Les acteurs de la Sécurité des Systèmes d'Information

a. 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».

A 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 Systhèmes d'Information et de Télécommunications ;
- 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 pour la communauté du supérieur.

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.

b. 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 devra 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 réalisée par système ou par domaine (GRH, concours, …).

2.3 Règles d'usages des systèmes d'information

Elaborés pour servir les missions éducatives de gestion du ministère de l'Éducation nationale ainsi que celles des collectivités territoriales dans le cadre des lois de décentralisation, les systèmes d'information sont accédés et exploités par une population d'utilisateurs essentiellement internes.

Néanmoins, à moyen terme, ceux-ci seront ouverts, conformément aux dispositions législatives et aux textes en vigueur, à de nouvelles catégories d'utilisateurs externes.
Aussi, pour pouvoir élaborer de nouvelles règles d'accès sécurisé, il convient au préalable de bien cerner et recenser les populations d'utilisateurs réels ou en situation de le devenir.

Sont ainsi identifiés en tant que tels, les apprenants (élèves, étudiants), les personnels toutes catégories confondues, les parents d'élèves (en qualité d'individus ayant-droits), les collectivités territoriales, les corps de contrôle, les organisations représentatives (des parents, des personnels, des élèves ou autres), les partenaires (financiers, institutionnels, etc.), les exploitants des systèmes d'information (Webmaster, directeurs de publication, administrateurs réseaux et systèmes, administrateurs de bases données et autres), les responsables de la sécurité des systèmes d'information ainsi que d'autres utilisateurs dont la liste exhaustive ne peut être établie précisément.

Chacun, à son niveau, doit être sensibilisé aux problématiques de la sécurité des systèmes d'information et se doit de participer à l'application des règles qui auront été définies.

Le **Brevet Informatique Internet (B2I)** constitue à cet égard une sensibilisation de premier niveau des élèves à la notion de sécurité des systèmes d'information.

Le **Certificat Informatique Internet (C2I)** constitue aussi une sensibilisation de premier niveau des étudiants à la notion de sécurité des systèmes d'information.

Enfin, et toujours dans le même esprit, ont été élaborées plusieurs chartes nationales de sécurité destinées à sensibiliser les élèves et personnels du ministère de l'Éducation nationale (utilisateurs et administrateurs réseaux).

De ce fait, elles constituent les droits et devoirs de chacun des usagers internes ou externes des systèmes d'information de l'institution.

2.3.1 La charte pour les personnels de l'Éducation nationale

Cette charte de référence a été élaborée et mise au point pour encadrer les conditions d'utilisation des ressources informatiques et systèmes d'information de l'institution par les personnels du ministère de l'Éducation nationale.

Exerçant une activité professionnelle au sein d'une entité relevant de la responsabilité d'une PJR, **les personnels et autres intervenants** (professionnels, associatifs...) se doivent de respecter la réglementation en général et tout particulièrement les règles de déontologie et de sécurité consignées dans la charte d'utilisation des ressources informatiques dont les PJR doivent assurer la diffusion.

En tant qu'utilisateur et/ou personnel de l'état, chaque individu est responsable en tout lieu et tout temps de l'usage qu'il fait des ressources informatiques, des réseaux ou des systèmes qui sont mis à sa disposition.

2.3.2 La charte nationale élèves

Cette charte de référence a été élaborée et mise au point pour encadrer et clarifier les conditions d'utilisation par les élèves, des ressources informatiques pédagogiques de l'institution.

La sécurité des systèmes d'information de l'institution et des établissements repose avant tout sur l'adhésion de l'ensemble des acteurs du dispositif, usagers et représentants légaux. Principale catégorie d'usagers de par leur nombre, les élèves se doivent de respecter les lois en vigueur, les règles de sécurité et de déontologie édictées par l'entité, au travers d'une charte de bon usage des ressources utilisées.

À partir de la charte nationale élève type, une charte doit être élaborée au sein de chaque entité, afin d'assurer son appropriation par l'ensemble de la communauté éducative. Cette charte ainsi élaborée devra avoir valeur de règlement intérieur.

Le ministère met à disposition des entités un guide méthodologique d'élaboration de la charte de bon usage des ressources TIC, ainsi qu'une charte de référence et des exemples concrets de chartes déjà élaborées par d'autres établissements.

Cette phase de mise en place de la charte devra s'accompagner de mesures de sensibilisation pédagogique et de formation des élèves à la problématique de sécurité des systèmes d'information notamment au travers du B2I (Brevet Informatique Internet) pour les élèves et le C2I (Certificat Informatique Internet) pour les étudiants.

2.3.3 Les utilisateurs externes et la sécurité des systèmes d'information

Dans le cadre du développement de la dématérialisation des documents et de la mise en œuvre de téléservices, les Espaces Numériques de Travail (ENT) sont mis en œuvre.

Cela se traduit notamment par une ouverture massive des systèmes d'information à des usagers externes au système éducatif (usagers ayant-droits, utilisateurs institutionnels, etc.).

Ces ouvertures ne peuvent s'opérer sans mise en place d'un cadre organisationnel de la sécurité des systèmes d'information.

C'est pourquoi il convient d'informer ces usagers des normes et règlements auxquels ils sont soumis dans le cadre de l'utilisation des systèmes d'information du ministère de l'Éducation nationale depuis l'extérieur de l'institution (partenaires) ou de l'intérieur (parents d'élèves). Ils sont également informés des réglementations relatives à la protection de la vie privée des personnes, des droits moraux et patrimoniaux découlant de la propriété intellectuelle, à la protection des systèmes d'information, etc.

Certains usagers des systèmes d'information sont tenus à une clause de confidentialité qu'ils doivent accepter avant tout exercice de mission au sein de l'institution.

L'ensemble des règles et orientations relatives à la sécurité des systèmes d'information déclinées plus haut devra être formalisé plus précisément au niveau de chaque entité ou établissement dans un Plan de Sécurité des Systèmes d'Informationappelé par convention P2SI.

2.4 Plan de sécurité des Systèmes d'Information (P2SI)

Soumis à une très grande dispersion géographique avec un grand nombre d'établissements intervenant à tous les niveaux pédagogiques du primaire au supérieur, le système éducatif rencontre **une multitude de configurations de fonctionnements et d'infrastructures.**

C'est pourquoi les contraintes de sécurité ne peuvent être appliquées de façon identique dans chacune de ces organisations, notamment

en raison des différences de niveau d'équipement en ressources informatiques mais également en raison de la variété des besoins d'accès aux systèmes d'information de l'institution.

Néanmoins, **l'enjeu de la sécurité doit rester identique pour l'ensemble des services du ministère de l'Éducation nationale**, même si des solutions techniques et organisationnelles particulières peuvent apparaître comme distinctes d'une entité à l'autre (école, établissement scolaire du second degré, établissement d'enseignement supérieur, services académiques, administration centrale ou autres établissements).

Il s'agit donc de **rendre cohérent les dispositifs de sécurité des systèmes d'information** déployés dans les entités par l'élaboration de Plans de Sécurité des Systèmes d'Information dénommé P2SI conformes au «Cadre Commun de la Sécurité des Systèmes d'information» annexé au SDS SI.

L'établissement du P2SI relève de la responsabilité de la «Personne Juridiquement Responsable». La PJR s'appuie sur les personnes compétentes en matière de sécurité au niveau local (RSSI, Correspondants de Sécurité, …) mais également en sollicitant l'assistance du pôle d'expertise «Sécurité des Systèmes d'Information» mis en place au niveau national.

Chaque entité dispose de son propre P2SI adapté à ses spécificités. Le P2SI est évalué par le niveau immédiatement supérieur avant de soumettre une demande d'inscription au registre des P2SI. S'agissant des établissements, le P2SI, présenté par la PJR, est soumis aux Conseil d'Administration et autorités des tutelles. Le P2SI est réactualisé en tant que de besoin en liaison avec les évolutions du Schéma Directeur de la Sécurité des systèmes d'information.

La cohérence globale des Plans de Sécurité (P2SI) avec les orientations générales de la Sécurité des Systèmes d'Information sera admise dès lors que celui-ci sera publié au registre national des P2SI.

Le registre des P2SI est matérialisé par une application collaborative ouverte aux acteurs concernés et gérée par un centre d'expertise spécialisé.

3. Mise en œuvre opérationnelle

La mise en œuvre opérationnelle des dispositifs de sécurité nécessite des décideurs, un engagement fort et un travail en étroite coordination avec les responsables techniques dans la mesure où il leur revient d'impulser des actions de natures différentes qui recouvrent aussi bien la sensibilisation aux risques et enjeux de la sécurité des SI que la détermination des moyens techniques et des technologies susceptibles de répondre à l'évolution de ces risques.

Différentes actions ont déjà été entreprises en ce sens, que ce soit par le biais d'une mise en place d'un réseau de compétences permettant de créer des chaînes d'alertes (RSSI, ISR ou CT du CERT RENATER) ou par l'élaboration d'un cadre de référence pour la mise en réseaux des établissements (S2I2E).

Ces actions doivent s'inscrire dans la durée et être complétées notamment par des dispositifs techniques renforcés décrits dans les § 3.2.1 et § 3.2.2 afin que les personnels, élèves et parents mais aussi tout type de partenaires (collectivités territoriales, entreprises…) puissent accéder aux réseaux de l'Éducation nationale sans mettre en danger la sécurité globale des SI.

Aussi, la mise en œuvre de ces quelques actions tend à prouver que la sécurité des systèmes d'information est déjà pour partie prise en compte dans les services de l'Éducation nationale mais qu'elle doit se développer davantage, notamment au travers des actions précisées ci-dessous.

3.1 La sensibilisation à la sécurité

Les dispositifs de sécurité ne peuvent être efficients que s'ils sont perçus comme des bénéfices et non vécus comme des contraintes.

Pour cela, un apprentissage minimal de la SSI d'ensemble est nécessaire. Divers moyens doivent être utilisés pour y parvenir :

- Formation des élèves et étudiants au travers, respectivement, du Brevet Informatique et Internet (B2I) et du Certificat Informatique et Internet (C2I).
- Séminaires de sensibilisation et formation des décideurs, «Personne Juridiquement Responsable» et «Autorités Qualifiées pour la Sécurité des Systèmes d'Information».
- Communications sur la sensibilité d'une application à destination des personnels du ministère de l'Éducation nationale.
- Mise en place de points d'informations à chaque échelon hiérarchique.
- Formation des maîtrises d'ouvrages, maîtrises d'œuvres, RSSI, Correspondants Techniques et Correspondants de Sécurité (notamment à la gestion des risques SSI).

Parallèlement à ces actions, la charte d'utilisation des ressources et de bon usage des systèmes d'information doit être diffusée aux personnels pour leur signifier leurs droits et devoirs en la matière.

3.2 Les moyens techniques de sécurité

Sur le plan technique, il convient tout d'abord de rappeler que la protection des systèmes d'information a toujours été une préoccupation de tout instant des informaticiens. Cependant, celle-ci est essentiellement réalisée par le biais des dispositifs de protection de l'infrastructure réseau. Il est en effet assez aisé d'y apporter un niveau de sécurité acceptable : la protection des systèmes est ainsi centrée sur les ressources.

Or, l'ouverture des systèmes d'information, jusqu'à présent cantonnée aux seuls utilisateurs présents et identifiés sur le réseau de communications, devient un **enjeu majeur du ministère de l'Éducation nationale** autant pour les personnels dont les postes de travail se banalisent que pour les utilisateurs externes (extranet).

Dès lors, il s'agit d'organiser la sécurité des systèmes d'information sur un système centré sur l'utilisateur afin de lui offrir un accès simple et sécurisé aux services dont il a besoin dans le cadre de son travail ou de ses échanges au sein de l'institution.

Cette démarche implique de préserver les principes de sécurité déjà mis en place dans le cadre d'un système centré sur les ressources, tout en lui adjoignant des principes de sécurité supplémentaires liés à la reconnaissance de l'individu.

3.2.1 Une architecture sécurisée

La tentative d'intrusion à l'un des quelconques constituants du Système d'Information de l'Éducation nationale ne doit pas conduire à mettre en péril la sécurité de l'ensemble des services offerts par celui-ci.

Aussi, afin de restreindre les risques de propagation d'une menace sur l'ensemble de l'infrastructure réseau de l'Éducation nationale, la mise en place des règles de confinement doit permettre de limiter ce risque.

Les règles de confinement sont celles étant définies comme des regroupements logiques de composants techniques de l'infrastructure réseau. L'établissement des zones de confiance correspond à un périmètre de protection maîtrisé.

Les échanges de flux entre les zones de confiance sont régis par des règles contenues dans un référentiel de sécurité.

Chaque référentiel de sécurité doit être cohérent avec la politique de sécurité des systèmes d'information de l'entité.

3.2.2 Les identités numériques

Pour pouvoir ouvrir l'accès d'un site ou d'une zone de confiance à d'autres usagers que les seules personnes présentes sur ledit site, la reconnaissance des individus en tant que tels devient impérative.

Deux moyens de preuve d'identité se distinguent :

- L'identification qui permet à un utilisateur de déclarer quelle identité numérique il va utiliser par exemple le numen, l'adresse email, etc.
- L'authentification faible ou forte qui permet à un utilisateur de prouver que l'identité numérique utilisée est bien la sienne par exemple mot de passe - code d'accès à un support de type carte - carte à puce - clé matérielle (USB ou autre) – voire empreinte digitale, rétinienne ou tout autre dispositif.

L'authentification constitue le facteur clé de la reconnaissance d'un individu et des contrôles d'accès associés. De sa qualité et de sa robustesse dépendent la protection des systèmes d'information.

En complément, la propagation de l'identité de l'utilisateur lui confère un accès unifié et transparent à l'ensemble des services et SI de l'Éducation nationale.

La signature électronique à base de certificats stockés sur un support externe du type carte «agent» contribue notamment à une authentification forte des personnes.

Ce dispositif, dans un contexte d'exploitation sécurisée définie par la politique de certification du ministère, permet également de signer numériquement des documents ou toutes autres ressources électroniques en contribuant à leur dématérialisation. Cette

signature électronique assure à la fois l'intégrité des données et l'authentification de la personne qui les a signées.

3.2.3 L'autorisation et les droits d'accès

L'autorisation (gestion des droits) consiste à accorder à une identité numérique des droits d'accès correspondant à son profil ou à ses missions (rôles).

Cette gestion des droits doit s'accompagner d'une gestion de délégation afin que chaque responsable d'une mission puisse déléguer vers ses collaborateurs les autorisations nécessaires à l'accomplissement de ses missions.

Les principes de l'authentification et de l'autorisation seront mis en œuvre dans le cadre des Espaces Numériques de Travail (ENT) mis à la disposition des établissements.

3.2.4 La protection des accès Internet

L'usage de l'Internet dans les pratiques éducatives est déjà très largement développé et se banalise progressivement avec le déploiement généralisé des accès. Cette banalisation des accès et des usages doit bénéficier de mesures d'accompagnement adaptées, destinées à faciliter le travail des équipes pédagogiques, tout en prenant en compte des impératifs de sécurité et notamment **la protection des mineurs et l'intégrité du réseau.**

Différents types de situations peuvent se présenter lors de la navigation sur l'Internet :

- **l'accès à des contenus inappropriés dans le cadre éducatif.** Concrétisés principalement par l'affichage de contenu inapproprié, que ce soient des contenus répréhensibles vis à vis de la loi et de la protection des mineurs (pages pornographiques, racistes, etc.),

ou des contenus qui n'ont pas directement leur place dans le cadre éducatif ;

- **les menaces visant l'intégrité du réseau**
  Se manifestant principalement par des attaques virales ainsi du code malveillant présent dans des pages visitées et dont l'objectif final est souvent le vol des données ;
- **l'accès à des contenus inappropriés dans le cadre professionnel**
  Concrétisés principalement par l'affichage de contenu inapproprié, que ce soient des contenus répréhensibles vis à vis de la loi ou des contenus qui n'ont pas directement leur place dans le cadre professionnel.

La mise en place d'un dispositif de contrôle ou de sélection, comme cela a été fait pour les courriers électroniques, doit être effectuée également sur l'accès à l'Internet. L'établissement ou le service doit identifier les besoins, définis et validés par l'institution, exprimés par l'ensemble des acteurs, et choisir un dispositif qui permette de répondre aux impératifs de sécurité tout en prenant en compte les besoins des acteurs et des usagers.

Une liste noire nationale de sites inappropriés est mise à disposition des communautés éducatives. Les documents d'accompagnement et leurs évolutions sont tenus à jour sur un site de référence.
La PJR est chargée de veiller à la mise en œuvre du dispositif.

3.2.5 La traçabilité

Tracer l'activité des systèmes d'information est primordial pour une organisation. L'exploitation des traces, qui doit être déclarée à la CNIL, doit permettre :

- De détecter les attaques, les activités inhabituelles ou inappropriées qu'elles soient d'origine interne ou externe.
- la «Personne Juridiquement Responsable» ainsi que le Responsable de Sécurité des Systèmes d'Information doivent avoir à leur disposition le bon niveau de traces.

- De déterminer l'étendue d'une intrusion éventuelle afin de la circonscrire.
- D'aider à la conduite d'enquête concernant les attaques détectées afin de pouvoir les neutraliser définitivement.

3.2.6 Le plan de sauvegarde et de secours

Un plan de secours s'impose pour assurer **le maintien d'une activité minimale pour les services vitaux.**

Le plan de sauvegarde doit être prévu et les supports doivent être hébergés en lieu sûr.

Le plan de secours se compose :

- D'un plan de reprise dans lequel sont décrites **les responsabilités et les opérations** qui doivent être menées pour continuer d'assurer les services et garantir le fonctionnement des ressources critiques de l'infrastructure informatique jusqu'au retour normal des conditions d'exploitation.
- D'un plan de continuité dans lequel sont décrites les opérations qui doivent être menées en cas de crise pour assurer la continuité de l'activité.

3.2.7 La sécurité physique

Il est nécessaire de protéger physiquement le système d'information contre **des évènements volontaires ou accidentels préjudiciables** tels que : vol, destruction de support, …, et également contre l**es risques dits «naturels»** : incendie, dégâts des eaux, foudre, coupure d'énergie, défaillance du circuit de climatisation, etc.

Les ressources sensibles, requérant donc une protection renforcée, seront protégées en fonction de leur sensibilité par les moyens physiques adéquats.

Des recommandations sur l'urbanisation et la mise en sécurité des salles machines sont disponibles dans le livre blanc «urbanisation et sécurisation des salles machines».

4. Plan d'actions 2004-2007

Pour être efficace, les grandes orientations du SDS SI du ministère de l'Éducation nationale doivent être soutenues à tous niveaux, notamment par la mise en œuvre d'un plan d'actions dont les premiers éléments sont précisés ci-dessous.

Issu des réflexions du comité opérationnel de la sécurité, ce plan d'actions ne doit en aucun cas être considéré comme exhaustif et susceptible de répondre à l'ensemble de la problématique.

4.1 Renforcer le dispositif de formation et d'information

Pour accompagner la démarche du Schéma Directeur de la Sécurité des Systèmes d'Information, la sensibilisation et la formation des décideurs des différents niveaux du système éducatif ainsi que celles des spécialistes, sont fondamentales notamment pour obtenir leur adhésion. De ces actions réussies dépendra la bonne mise en œuvre du Schéma Directeur de la Sécurité des Systèmes d'Information : la formation doit permettre entre autre une forte sensibilisation des utilisateurs à la notion de chaînes d'alerte.

Le programme de formation est personnalisé pour les cibles suivantes :

- les décideurs ;
- les maîtrises d'ouvrage ;
- les spécialistes des systèmes d'information ;
- les RSSI ;
- les utilisateurs.

a. Mettre en place des séminaires de sensibilisation des décideurs et des personnels d'encadrement des services académiques et établissements d'enseignement.

Action

- Validation finale du dispositif avec une déclinaison du séminaire académie par académie dès 2004. L'organisation du séminaire devra fédérer toutes les communautés éducatives (scolaire et supérieur).
- Annexion au SDS SI d'une proposition de contenu.

Coordination

- DPMA-DT-DR (notamment au travers de la cellule technique du CRU)

b. Mettre en place de séminaires de sensibilisation des établissements.

Action

- Elaboration courant 2004 d'un dispositif complémentaire de sensibilisation à destination des chefs d'établissement du scolaire.
- Annexion au SDS SI d'une proposition de contenu.

Coordination

- DPMA-DT-DE

c. Informer les différents acteurs de la mise en place de chartes nationales régissant l'usage des TIC.

Action

- Validation officielle des chartes régissant l'usage des TIC.
- Annexion au SDS SI, des chartes relatives aux élèves, personnels et administrateurs de systèmes d'information.
- Diffusion généralisée des chartes pour annexion au règlement intérieur des services et établissements.
- Formalisation d'un plan de communication adapté.

Coordination

- DPMA-DT-DESCO-DR (notamment au travers de la cellule technique du CRU).
- Autres directions associées : DPE et DE.

4.2 Mise en œuvre du carnet de sécurité pour toutes les applications

Action

- Mise en place du carnet de sécurité pour tout système d'information. Ce carnet comprend notamment :
  - l'expression de besoins fournie par la MOA,
  - le cahier de spécifications fourni par la MOE,
  - le dossier CNIL, les consignes d'exploitation…
- Ouvert à tous les acteurs concernés, le carnet de sécurité est matérialisé par une application collaborative de type «suivi de processus».
- Accompagnement des MOA dans l'expression des besoins en matière de sécurité (mise en œuvre d'une méthodologie appropriée propre à l'Éducation nationale et dérivée d'EBIOS).

Coordination

- DPMA en partenariat avec toutes les maîtrises d'ouvrage.

4.3 Renforcer la cohérence entre les politiques de sécurité des systèmes d'information

Malgré la diversité des composantes du système éducatif, le Cadre Commun de la Sécurité des Systèmes d'Information constitue la référence pour **l'élaboration des Plans de Sécurité des Systèmes d'Information.**

Action

- **Accompagnement des services et des établissements dans la définition de leur Plan de Sécurité des Systèmes d'Information (P2SI)** sur la base du cadre commun de sécurité annexé au SDS SI et des plans types de sécurité.
- Mise en place d'un **dispositif de consolidation et d'évaluation des PSI par sphère** (services académiques, EPLE, établissements du supérieur, ...)

- Constitution d'**une cellule nationale de conseil.**
- Mise en place d'**un registre national des P2SI.**

Coordination

- DPMA-DT-DR (notamment au travers de la cellule technique du CRU)

4.4 Mettre en place et animer une chaîne de responsabilités et d'alerte.

L'établissement d'une chaîne opérationnelle de responsabilités a pour objectif :

- de piloter, superviser et contrôler l'ensemble des opérations ayant trait à la sécurité des systèmes d'information ;
- de déléguer les responsabilités au niveau local pour prendre en compte les spécificités de chaque organisation ;
- d'assurer la cohérence globale de la sécurité des systèmes d'information en instituant une méthodologie commune.

Action

- Mise en place opérationnelle des RSSI dans les académies (enseignement scolaire).
- Publication au Bulletin Officiel de l'Education Nationale (BOEN) de la liste des Responsables académiques de la Sécurité des Systèmes d'Information (RSSI) nommés dans chaque académie par les recteurs et réactualisée chaque année.
- Organisation de l'animation du réseau des RSSI de l'enseignement scolaire et du supérieur afin :
  - de développer un socle organisationnel commun
  - de structurer les chaînes d'alerte
  - de déterminer les actions à entreprendre selon la nature des attaques ou incidents de sécurité
- Prise en compte de la chaîne PIRANET

Coordination

- DPMA-DT-DR (notamment au travers de la cellule technique du CRU)

4.5 Protéger l'élève et organiser le référencement de sites aux contenus illicites et inappropriés

Action

- Mise en place d'un dispositif global d'aide à l'utilisation de l'Internet dans le cadre pédagogique, qui s'appuie sur la sensibilisation, la formation et la responsabilisation de l'ensemble des usagers et acteurs ainsi que sur la mise en place de dispositifs techniques de sélection et de contrôle des sites consultés.
- Mise en place d'une cellule nationale de coordination : celle-ci sera informée par une chaîne d'alerte de tous les problèmes éventuels.
- Établissement d'une liste noire nationale de sites inappropriés : une cellule spécialisée est chargée de la pérenniser et de la faire évoluer. En cas de besoin, une cellule d'aide psychologique nationale est disponible.
- Sensibilisation et formation des élèves par la mise en œuvre du B2I.
- Poursuite de l'équipement des écoles en dispositif de contrôle dans le cadre du projet S2I2E.

Coordination

- DT-DPMA

4.6 Rechercher la mutualisation des ressources et des moyens

Le développement de nouveaux services dans le cadre de la maîtrise des moyens doit prendre appui sur une plus grande mutualisation des ressources.

Ainsi, les établissements doivent pouvoir s'appuyer sur les services académiques, disposant des structures ad hoc (équipes de développement et d'exploitation), pour prendre en charge les services de base de la sécurité tels que la sauvegarde, l'hébergement de machine, la maintenance, la supervision ou l'exploitation dans le cadre d'une consolidation académique.

Sur ce même principe, la création d'un pôle de compétence de la Sécurité des Systèmes d'Information offre un service global à toutes les académies ou établissements scolaires.

Action

- Mise en place du pôle de compétence[1] de la Sécurité des Systèmes d'Information d'assistance à maîtrise d'ouvrage pour la SSI : il appuiera les services académiques et les EPLE dans leur approche sécurité par une offre de service en conseil, audit et veille technologique.
- Mise en place d'un Centre de Surveillance[2] et d'alerte : il offrira un service de supervision des infrastructures informatiques des systèmes d'information académiques hors temps ouvrable dans l'optique d'élever le niveau de disponibilité.
- Mise en place d'un Centre de Repli[2]: il permettra en cas de sinistre grave dans une académie, de reprendre dans un délai raisonnable les activités informatiques de l'académie concernée.

Coordination

- DPMA

4.7 Se donner les moyens d'élever le niveau global de sécurité

L'objectif est d'élever le niveau global de sécurité tout en offrant la plus grande ouverture des systèmes d'information notamment au

[1] Pôle de compétence d'Aix-Marseille
[2] Pôle de compétence de Nancy-Metz

regard de la pluralité des lieux de travail des acteurs. Il conviendra de compléter la sécurité basée essentiellement sur le cloisonnement des systèmes à une sécurité basée sur une authentification forte et individualisée (gestion des droits et profils) de l'usager.

Action

- Renforcer la sécurité dans les EPLE :
  Le déploiement des Services Internet/ Intranet dans les établissements et écoles (projet S2I2E) doit se poursuivre. Dans la circulaire NOR MENT0400337C du 18 février 2004 parue au Bulletin Officiel de l'Education nationale, le ministre indique qu'à terme l'ensemble des établissements et écoles disposera de tels services. Les équipements S2I2E intègrent des dispositifs de sécurité, tels que des pare-feu et des équipements de filtrage.
- Le réseau privé virtuel AGRIATES réunissant dans une même zone de confiance établissements et services académiques sera déployé.
- **Développer les moyens techniques**
  - Carte agent et signature électronique
    Les infrastructures de référence ont été déployées en 2004 (exploitées par le pôle de compétence de l'académie de Toulouse). Dans le cadre de la Nouvelle Gestion des Promotions, **10 000 agents disposent d'une signature électronique matérialisée par une clé USB appelée i-clé**. La poursuite du déploiement permettra de s'engager plus en avant dans la dématérialisation des procédures et la banalisation des postes de travail en offrant un moyen de reconnaissance individuel pour les actions de signature et d'authentification.
  - La gestion de l'identité
    L'usager, qu'il soit élève, étudiant ou personnel de l'Éducation nationale, doit pouvoir accéder à son espace de travail et à toutes

les applications qui le composent au travers d'une identification unique et une gestion fine de son profil et de ses droits. **La gestion de l'identité doit être associée à une base de connaissance sûre et exhaustive : l'annuaire.**

La mise en place de la gestion de l'identité doit accompagner le développement des espaces numériques de travail. Le couplage de la signature électronique et de la gestion de l'identité est le gage d'une sécurité maîtrisée et individualisée.

- La traçabilité

Un effort particulier sera consacré à la fourniture d'outils de traçabilité à tous les niveaux du système éducatif.

Un projet de déclaration de gestion des traces sera établi et soumis à la CNIL.

Coordination

- DPMA-DT-DR (notamment au travers de la cellule technique du CRU)

4.8 Développer des outils d'évaluation et de pilotage de la mise en œuvre du SDS SI

Action

- Développement d'outils d'exploitation du registre des P2SI.
- Suivi et consolidation des actions de formation, de sensibilisation aux problématiques de sécurité.
- Établissement du bilan annuel de mise en application du SDS SI.
- Construction de tableaux de bord de suivi.

Coordination

- DPMA

5. Documents de références

Référentiels d'application

- Cadre commun de la sécurité
- Plans types de Sécurité des Systèmes d'Information (P2SI)

Chartes

- Charte élève
- Chartes des personnels de l'Éducation nationale
- Chartes des administrateurs des Systèmes d'Information et des infrastructures
- Annexe Juridique de l'utilisateur
- Guide Technique de l'utilisateur
- Guide méthodologique d'élaboration de la charte de bon usage des ressources TIC (charte élève)
- Déclaration type CNIL «mise en œuvre de traces»

Méthodologies

- Méthodologie d' Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) simplifiée

Formation

- Programme type de sensibilisation des décideurs à la sécurité des systèmes d'information

Recommandations

- Livres blancs
  - urbanisation des systèmes d'information
  - sécurité des salles informatiques
  - sécurité des procédures d'exploitation
- Référentiel de sauvegarde du ministère de l'Éducation nationale
- Services Intranet et Internet des Établissements et des Écoles (S2I2E)
- Recommandation interministérielle pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense (IG n° 901/DISSI/SCSSI du 2 mars 1994).