MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Cadre général de sécurité des services numériques pour l'éducation

Doctrine technique
du numérique pour l'éducation
Juillet 2024

Table des matières

1. Préambule

1.1. Contexte

Le présent document se place dans la démarche de la doctrine technique du numérique pour l'éducation dans son volet de sécurité numérique. Il s'agit de fournir à chaque acteur d'un dossier, selon ses prérogatives, un cadre général permettant d'opérer les actions requises afin de garantir la sécurité des services pour l'Éducation dans son ensemble, en lien avec les autres acteurs compétents et de manière cohérente avec l'ensemble de la doctrine.

D'une manière générale, chaque organisme – établissement, opérateur, direction des systèmes d'information – comme chaque type d'application, peuvent présenter des enjeux de sécurité qui lui sont spécifiques et en conséquence des mesures opérationnelles différentes. Néanmoins, la dématérialisation des procédures, l'interconnexion des différents systèmes d'information, la consommation des mêmes données par des systèmes hétérogènes, l'exposition sur Internet des télé-services, conjointement à la forte croissance des attaques informatiques, contribuent à faire de la sécurité numérique un enjeu global et partagé, qu'il est nécessaire de promouvoir de manière commune dans le contexte de la présente doctrine.

1.2. Objectifs du document

La sécurité numérique a pour objectif premier la mise en œuvre de mesures techniques, organisationnelles, procédurales pour assurer la protection des systèmes et des personnes. Les responsabilités des différents acteurs, qui partagent juridiquement et techniquement les compétences liées à la sécurité, sont à conjuguer avec subsidiarité.

En conséquence, la comitologie qu'il convient de mettre en place pour assurer le partage d'information est un axe essentiel à développer pour chaque périmètre au début de la démarche de conception des systèmes, permettant de mettre en lien les équipes locales et les équipes transversales.

D’un point de vue légal et réglementaire, les corpus de règles peuvent être communs à tous les acteurs (RGPD, EIDAS[1], SREN[2], codes spécifiques, etc.) ou différer sur la forme mais convergent sur le fond. Dès lors, au-delà de la lettre, c’est l’esprit de la doctrine, selon laquelle les efforts conjoints visent une sécurité globale, qu’il convient de promouvoir, chacun selon son périmètre et selon l’aspect réglementaire qui s’y exerce.

Ainsi, la loi n° 2013-595 d'orientation et de programmation pour la refondation de l'École de la République du 8 juillet 2013 est commune à chaque périmètre et rappelle dans ses dispositions que la maintenance et l’équipement informatique des établissements publics locaux d’enseignement (EPLE) sont à la charge des collectivités territoriales, à l’exception des services numériques contractualisés directement par le chef d’établissement. Dès lors, les aspects d'architecture informatique pour le périmètre des établissements, mais également pour les services mutualisés ainsi que les aspects d’exploitation des différents systèmes d’information, relèvent de la responsabilité des collectivités territoriales.

Les domaines de partage de connaissances et d’échange permettant de mutualiser les compétences en termes de sécurité numérique relèvent de cinq registres :

- les homologations des systèmes d’information ou des applications,
- les contrôles de sécurité ou audits suivant les référentiels techniques,
- les clauses de sécurité dans les marchés,
- la gestion d’incidents de sécurité numérique,
- la politique opérationnelle de sécurité numérique commune.

1.3. Cycle de vie du document et gouvernance

Le ministère et ses services déconcentrés ainsi que les collectivités territoriales ont participé à l’élaboration de ce cadre général.

Le présent document constitue la première version du cadre général de sécurité des services numériques pour l’éducation.

Une mise à jour annuelle du document est prévue à l’instar de la doctrine technique du numérique pour l’éducation.

[1] https://cyber.gouv.fr/le-reglement-eidas-n9102014

[2] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

2. Les règles de sécurité du numérique pour l'éducation composant la doctrine technique

2.1. Relativement aux homologations

Le ministère est tenu d'homologuer ses systèmes d'information et les services numériques qui y sont liés selon plusieurs référentiels et de fournir le corpus minimal pour permettre aux autorités d'engager les usagers à utiliser ces services sachant que la sécurité juste et adaptée a été évaluée par les comités compétents.

Plusieurs véhicules réglementaires le rappellent (RGS, PSSIE, instructions interministérielles ou ministérielles). Les autorités qualifiées pour la sécurité des systèmes d'information et les autorités d'homologation pour mener à bien ces chantiers sont nommés par voie réglementaire.

Les dossiers d'homologation intègrent l'aspect RGPD tant dans sa dimension d'inscription au registre que d'étude d'impact potentielle. Plus généralement, tous les acteurs impliqués dans la construction et l'exploitation des services numériques sont tenus par le RGPD.

À noter que le respect du RGPD emporte également – du fait des principes de minimisation des données manipulées qu'il met en exergue – les conditions de réduction de l'empreinte environnementale. Il paraît opportun de lier les deux concepts dans les travaux de manière à prendre en compte conjointement les attentes des deux domaines.

N°1	Règle
	Les autorités qualifiées de la sécurité des systèmes d'information mettent en place les homologations des services numériques qu'elles ont en responsabilité et invitent les services de sécurité compétents des autorités partenaires pour des partages d'information relativement aux commissions d'homologation.

2.2. Relativement aux contrôles de sécurité ou audits suivant les référentiels techniques

Concernant le contrôle de l'application des référentiels de sécurité publiés par l'ANSSI ou de la CNIL, il convient que les audits techniques soient élaborés de manière partagée entre les parties prenantes notamment les services techniques des collectivités et ceux de la région académique en vue de la tenue d'une commission d'homologation où chacune des parties est représentée.

Ces audits réguliers sont à la fois versés au dossier des commissions d'homologation et sont également une opportunité pour améliorer conjointement le niveau de sécurité des systèmes d'information contribuant à l'offre de services numériques pour l'éducation.

N°2

Règle

Les audits techniques des services numériques pour l'éducation sont conçus et réalisés de manière conjointes par les équipes techniques académiques et celles des partenaires ainsi que des acteurs tiers intervenant dans l'offre de services. Ces équipes pourront mandater conjointement des audits externes par prestation le cas échéant. Un document socle précisant les points de contrôle et d'audit minimaux et commun à toutes les entités opérant sur les systèmes d'information offrant des services numériques pour l'éducation sera prescrit par un groupe de travail regroupant des différents acteurs du domaine.

2.3. Relativement aux clauses de sécurité dans les marchés

L'élaboration des services numériques pour l'éducation, lorsqu'il passe par des prestations mises en places suite à des marchés publics, doit prendre en compte les règles réglementaires relatives à la sécurité des systèmes d'information dès la rédaction du cahier des charges de manière à ce que l'exécution du marché puisse permettre aux équipes en charge de la mise en œuvre de commander les prestations adéquates. Dès lors, le partage d'information préalable concernant les clauses de sécurité des systèmes d'information dans les travaux de rédaction des cahiers des charges s'avère essentiel pour le bon déroulé du marché par la suite.

Ces efforts conjoints permettent notamment de faire converger les bonnes pratiques en matière de sécurité des systèmes d'information édictées par voies légale ou réglementaire s'appliquant dans les différents périmètres d'action des acteurs des services numériques pour l'éducation.

N°3

Règle

Les clauses de sécurité dans les marchés font l'objet d'une élaboration conjointe entre les équipes techniques à l'œuvre pour la construction des services du numérique pour l'éducation de manière à disposer des conditions d'exploitation sécurisée dans toutes les prestations existantes.

2.4. Relativement à la gestion d'incidents de sécurité numérique

Le traitement des incidents de niveau majeur relève d'un traitement conjoint entre les RSSI académiques, qui sont en charge du signalement des incidents de sécurité numérique auprès du centre opérationnel de la sécurité des systèmes d'information du ministère (Cossim), et les RSSI des collectivités territoriales.

Chaque chef d'établissement, sans être AQSSI, constitue le point de contact de la sécurité numérique pour les services déconcentrés de l'éducation nationale et particulièrement pour la chaine d'alerte du périmètre dont il est usager ou dont il a la responsabilité, notamment en cas d'incident de sécurité du numérique qui affecte fortement les activités de son établissement.

Pour ce faire, chaque académie maintient un annuaire des points de contacts en EPLE.

Le RSSI académique informe et prend l'assistance du Cossim de manière à ce que l'information soit traitée dans le contexte global des incidents touchant le ministère et en lien avec les autorités décisionnelles du ministère, en lien également avec l'ANSSI et les forces de l'ordre si nécessaire.

Il est essentiel que les échelons décisionnels du ministère soient en parfaite connaissance des incidents de sécurité survenant sur l'ensemble des services du numérique pour l'éducation dès leur survenance afin de pouvoir gérer les impacts de ceux-ci, diffuser l'information de nouvelles menaces à l'ensemble des acteurs des SI, qu'ils soient dans le périmètre lié aux ressources numériques pour l'éducation ou dans des périmètres connexes, y compris les équipes des collectivités territoriales pour leur propres besoins.

Il est primordial de faire cause commune dans le traitement et la gestion des incidents tant la rapidité de réaction vis-à-vis de nouveaux scénarios d'attaques est la clé pour limiter l'impact de ces attaques voire pour contrer totalement les tentatives grâce à la prévention ou la sensibilisation de l'ensemble des acteurs.

N°4	Règle Les incidents de sécurité doivent faire l'objet de déclarations aux chaines d'alerte adéquate selon les fiches de remontée d'incident diffusées à l'ensemble des acteurs des services numériques pour l'éducation.

2.5. Relativement à une politique opérationnelle de sécurité numérique

La définition de politiques opérationnelles a été l'objet de nombreux travaux sectoriels (par domaines industriels, administratifs, métiers, spécialités) et a permis de clarifier pour tous les acteurs concernés ce qui est attendu et à l'état de l'art tant dans l'élaboration des architectures que dans l'exploitation des systèmes d'information ou que dans les développements d'applications.

Dans la gestion partagée des traitements de données dans les services du numérique pour l'éducation, les interconnexions des systèmes d'information par interfaçage des différents périmètres conduisent à traiter conjointement les évolutions en fonction des besoins, des spécifications, mais également des remédiations consécutivement aux incidents et aux alertes. Il convient donc de définir un cadre qui puisse guider tous les acteurs dans la construction des services numériques à venir ou dans la conduite de ceux existant.

Un tel cadre général sera revu régulièrement par une comitologie constituée des acteurs de la filière du numérique pour l'éducation et des acteurs de la sécurité des systèmes d'information et soumis à validation au comité des partenaires.

N°5

Règle

Les équipes techniques des domaines liés au numérique pour l'éducation établissent conjointement, en lien avec les équipes de la sécurité numérique du ministère et des collectivités territoriales, une politique opérationnelle de la sécurité numérique (POSN) définissant un corpus de règles techniques à respecter dans la construction, l'exploitation et l'organisation du service numérique pour l'éducation de manière sécurisée.

3. Mise en application : les textes de référence

La démarche de sécurisation des systèmes d'information comme toutes les procédures de sécurité numérique s'adossent à des textes législatifs ou réglementaires les encadrant.

Pour rappel, sont listés ci-dessous les textes suivant les différents périmètres, sachant que ces corpus convergent vers les attentes de la doctrine rappelées plus haut.

Cadre réglementaire général s'appliquant aux services et infrastructures numériques opérés par le ministère, ses services déconcentrés et les établissements publics relevant de la tutelle ministérielle et des prestataires y intervenant

Les textes relatifs au numérique, à la sécurité du numérique et des systèmes d'information et de communication s'appliquant aux ministères, services déconcentrés et établissements publics relevant de la tutelle du ministère sont les suivants :

- Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics (NOR : PRMD2135717D).
- Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics (NOR : PRMD2221955A).
- Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique (NOR : PRMG1929496D).
- Le référentiel général de sécurité pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : PRMX0909445D).
- Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (NOR : PRMD1413745A).
- Circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'État (PSSIE) (NOR : PRMX1420095C).
- Instruction interministérielle n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles (NOR : PRMD1503279J).

- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : ECOX0500286R).
- Ordonnance n° 2017-1426 relative à l'identification électronique et aux services de confiance pour les transactions électroniques (NOR : PRMD1724021R).

Textes relatifs à la protection des données personnelles

- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (NOR : JUSC1732261L).
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment son article 85 et ses articles 140 et suivants (NOR : JUSC1911425D).

Textes concernant des périmètres spécifiques

- Arrêté du 13 juillet 2020 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Recherche publique » (NOR : PRMD2018060A) et leurs annexes.
- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information de services essentiels (NOR : PRMD1809740D).
- Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (NOR : PRMD1824939A).
- Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation (NOR : PRMX1118649D).
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation (NOR : PRMX1227979A).
- Circulaire interministérielle n° 3415/SGDSN/AIST/PST du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation (NOR: PR1vID1238889C).

Texte relatif à la protection du secret de la défense nationale

- Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (NOR : PRMD2123775A).

Texte relatif à l'organisation gouvernementale pour la gestion de crises majeures

- Circulaire n° 6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion de crises majeures.

Cadre réglementaire général s'appliquant aux services et infrastructures numériques opérés par les collectivités territoriales et des prestataires y intervenant

L'ANSSI a rappelé dans le document « Sécurité numérique des collectivités territoriales[3] » qui précise la nécessité de tenir des homologations ainsi que le respect du RGPD.

Ainsi, les textes relatifs au numérique, à la sécurité du numérique et des systèmes d'information et de communication s'appliquant aux services et infrastructures numériques opérés par les collectivités territoriales et les prestataires reprennent notamment les lois ou règlements suivants :

Textes relatifs au numérique, à la sécurité du numérique et des systèmes d'information et de communication

- Le référentiel général de sécurité pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : PRMX0909445D).
- Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (NOR : PRMD1413745A).
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : ECOX0500286R).

[3] https://cyber.gouv.fr/sites/default/files/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf

- Ordonnance n° 2017-1426 relative à l'identification électronique et aux services de confiance pour les transactions électroniques (NOR : PRMD1724021R).