

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA CULTURE

Arrêté du 21 janvier 2022 portant approbation de la politique de sécurité du numérique du ministère de la culture

NOR : MICB2201459A

La ministre de la culture,

Vu le code de la défense, notamment ses articles L. 2321-1 et R. 1143-1 à R. 1143-8 ;

Vu la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 portant la politique de sécurité des systèmes d'information de l'Etat ;

Vu la circulaire du Premier ministre n° 6290/SG du 15 juillet 2021 relative aux actions à engager pour renforcer la cybersécurité de l'Etat,

Arrête :

Art. 1^{er}. – La politique de sécurité du numérique du ministère de la culture, ci-après annexée, est approuvée.

Art. 2. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 21 janvier 2022.

ROSELYNE BACHELOT-NARQUIN

ANNEXE

POLITIQUE DE SÉCURITÉ DU NUMÉRIQUE DU MINISTÈRE DE LA CULTURE

POLITIQUE DE SECURITE DU NUMERIQUE (PSNUM) DU MINISTERE DE LA CULTURE

Décembre 2021



1. Introduction

La transformation numérique et l'ouverture croissante des systèmes d'information du ministère de la culture aux citoyens et aux partenaires rendent nos infrastructures et nos applications plus vulnérables aux cybermalveillances. Depuis plus d'une décennie, **une recrudescence des cyberattaques** à l'encontre des entreprises et organismes publics a été relevée en France et dans le monde. Tout particulièrement, les cybercriminels profitent des périodes de crise comme celle liée à l'épidémie Covid, pour envoyer de faux courriels d'alerte piégés contenant des rançongiciels.

Compte-tenu de ces menaces, **la sécurité du numérique ne doit plus être un domaine réservé aux seuls spécialistes**. Aussi chaque responsable d'administration et d'établissement public doit évaluer le risque numérique au même titre que les autres risques et consacrer les ressources humaines, budgétaires et techniques suffisantes pour les couvrir.

Pour faire face à ces enjeux de sécurité, qui croisent ceux liés à la **continuité d'activité**, à la **protection des données personnelles et du secret**, les organisations ont entrepris une démarche visant à rester résilients face à ces événements redoutés. Dans cet objectif, et en conformité avec l'instruction relative à la gouvernance de la sécurité numérique de l'Etat (2021), le ministère de la culture a élaboré sa propre **politique de sécurité du numérique (PSNum)** en déclinaison des réglementations interministérielles et européennes et en tenant compte de ses propres enjeux.

La **politique de sécurité du numérique (PSNum)** est un document présentant les **orientations stratégiques** portées par le ministère de la culture en matière de sécurité numérique. Cette instruction spécifie également les règles et les grands principes de sécurité qui devront être respectés et déclinés opérationnellement.

Les différentes sections décrivent :

- le **périmètre d'application** de la Politique de Sécurité du Numérique du ministère ainsi que le cadre réglementaire sur lequel elle s'appuie ;
- les **enjeux et les orientations stratégiques** retenues par le ministère en matière de sécurité du numérique pour faire face aux menaces actuelles ;
- les **instances de gouvernance de la sécurité du numérique**, ainsi que les **rôles et les responsabilités** associés à cette **gouvernance** pour les administrations centrales, les services à compétence nationale, les services déconcentrés et les établissements publics sous tutelle
- les **règles et processus de sécurité numérique** essentiels pour l'atteinte d'un niveau de sécurité conforme aux enjeux du ministère.

Table des matières

1. Introduction
2. Périmètre et cadre réglementaire
 - 2.1. Périmètre
 - 2.2. Cadre réglementaire
3. Enjeux et stratégie de la sécurisation du numérique
 - 3.1. Contexte lié à la sécurité du numérique
 - 3.2. Enjeux liés à la sécurité du numérique
 - 3.3. Principales menaces liées à la sécurité du numérique
 - 3.4. Stratégie de sécurisation numérique du ministère de la culture
4. Gouvernance ministérielle de la sécurité du numérique
 - 4.1. Rôles et responsabilités
 - 4.1.1. Le ministre
 - 4.1.2. Le haut-fonctionnaire de défense et de sécurité (HFDS) et par délégation le HFDS Adj
 - 4.1.3. Le fonctionnaire de sécurité des systèmes d'information (FSSI)
 - 4.1.4. L'autorité qualifiée en sécurité des systèmes d'information (AQSSI)
 - 4.1.5. Le conseiller à la sécurité du numérique (CSN)
 - 4.1.6. Le chef du service du numérique (SNUM)
 - 4.1.7. Le responsable de la sécurité des systèmes d'information (RSSI)
 - 4.1.8. Le responsable de la sécurité des systèmes d'information (DPD)
 - 4.2. Instances ministérielles de la sécurité du numérique
 - 4.2.1. Le comité ministériel de la sécurité du numérique
 - 4.2.2. Le comité de pilotage sécurité du numérique
 - 4.2.3. Le comité sécurité
 - 4.3. Sécurité du numérique dans les services déconcentrés
 - 4.3.1. Le responsable de la sécurité du numérique
 - 4.3.2. Le correspondant sécurité du numérique
 - 4.4. Sécurité dans les services à compétence nationale (SCN)
 - 4.4.1. Le responsable de la sécurité du numérique
 - 4.4.2. Le correspondant sécurité du numérique
 - 4.5. Gouvernance sécurité dans les établissements publics
 - 4.5.1. Le responsable de la sécurité du numérique
 - 4.5.2. L'organisation de la gouvernance
 - 4.5.3. Le point de contact relatif à la sécurité du numérique
 - 4.5.4. Mise en œuvre de la politique sécurité du numérique
 - 4.5.5. La déclaration des incidents de sécurité
 - 4.6. Relation entre le ministère et les autorités administratives
5. Règles et processus de sécurité du numérique
 - 5.1. Règles de sécurité
 - 5.2. Principaux processus de sécurité
 - 5.2.1. La cartographie des infrastructures, des applications et des données
 - 5.2.2. La classification des données par niveau de sensibilité
 - 5.2.3. La cartographie des risques

- 5.2.4. L'intégration de la sécurité dans les projets et les prestations
- 5.2.5. L'homologation
- 5.2.6. Le maintien en conditions de sécurité des infrastructures et des applications
- 5.2.7. La protection des données personnelles
- 5.2.8. La sensibilisation et la formation à la sécurité
- 5.2.9. La continuité d'activité
- 5.2.10. La gestion des dérogations
- 5.2.11. La veille sécurité des systèmes d'information
- 5.2.12. La supervision continue des infrastructures et des applications
- 5.2.13. La gestion des alertes et des incidents
- 5.2.14. La gestion de crise cybersécurité
- 5.2.15. Les contrôles
- 5.3. Corpus documentaire de la politique sécurité
- 6. Principales références
- 7. Glossaire
- 8. Annexes
 - 8.1. Missions des autorités qualifiées pour la sécurité des systèmes d'information (AQSSI)

2. Périmètre et cadre réglementaire

2.1. Périmètre

La **politique de sécurité du numérique** s'applique à l'ensemble des entités du **ministère de la culture** : administrations centrales, services déconcentrés, services à compétence nationale et aux établissements publics sous tutelle. Les établissements publics devront la décliner en fonction de leur contexte.

2.2. Cadre réglementaire

En conformité avec les **réglementations françaises et européennes**, le ministère de la culture a élaboré sa politique en tenant compte de ses enjeux et de ses besoins.

Ainsi, les principes ministériels de gouvernance que la présente politique décrit, doivent être conformes à l'instruction relative à la gouvernance de la sécurité numérique de l'Etat (2021). En outre, les règles de sécurité du numérique appliquées au sein du ministère doivent être cohérents avec la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

Par ailleurs, certains périmètres sensibles font l'objet d'exigences particulières :

- les services numériques participant à la gestion des informations et des supports classifiés doivent respecter l'**Instruction Générale Interministérielle 1300** (oct 2020) ;
- les systèmes d'information d'importance vitale doivent répondre aux articles de la **Loi de Programmation Militaire** ;
- les systèmes d'information mis en œuvre par le ministère dans ses relations avec les autres autorités administratives et avec les citoyens doivent respecter le **Référentiel Général de Sécurité** (RGS) ;
- les services numériques traitant des données à caractère personnel doivent être conformes avec le **Règlement Général sur la protection des données** (RGPD) ;
- enfin, les transactions électroniques et les systèmes d'authentification électronique doivent respecter le **règlement eIDAS** portant sur la confiance numérique.

3. Enjeux et stratégie de la sécurisation du numérique

La politique de sécurité du numérique définit des orientations stratégiques pour garantir la protection de ses ressources les plus sensibles face aux menaces.

3.1. Contexte lié à la sécurité du numérique

Le ministère s'est engagé dans une **transformation numérique** majeure avec notamment l'ouverture de nombreux services numériques pour les citoyens et la dématérialisation de l'ensemble des processus mis en œuvre pour ses agents.

Afin de garantir la qualité de ces services et leur souplesse d'usage, le ministère privilégie l'utilisation de l'informatique en nuage et des services en ligne, ainsi que la généralisation du télétravail.

Ces besoins engendrent une **ouverture croissante des systèmes numériques** du ministère aux acteurs externes, qu'il s'agisse de citoyens ou de partenaires. Cependant cette ouverture augmente de fait la surface d'exposition sur internet, propice aux attaques. Les services numériques du ministère doivent donc faire l'objet de mesures de sécurité afin de **préserver la confiance des usagers**.

3.2. Enjeux liés à la sécurité du numérique

Les travaux liés à la sécurité du numérique doivent se concentrer en priorité sur les services présentant des enjeux forts pour le ministère.

Ainsi, pour **protéger son patrimoine culturel numérique** et respecter la réglementation, notamment celle concernant la protection des données, le ministère doit garantir la confidentialité des données les plus sensibles, comme certaines gérées par les archives nationales ou les échanges entre les hautes autorités.

De plus, l'intégrité et la disponibilité des sites institutionnels et événementiels portés par le ministère doivent faire l'objet d'une attention particulière afin de protéger **l'image de l'institution** et de ses activités.

Enfin, dans le cadre de sa transformation numérique, le ministère doit garantir la disponibilité, la confidentialité et l'intégrité des **principaux services transverses permettant aux agents d'accomplir leurs missions** tels que les services bureautiques, la messagerie, les espaces partagés ou la visioconférence.

3.3. Principales menaces liées à la sécurité du numérique

La transformation numérique constitue un enjeu stratégique pour le ministère. Cependant le déploiement de nouveaux services est aussi **générateur d'opportunités pour les attaquants** aux profils et aux objectifs très variés.



La principale menace visant le ministère est l'**attaque par rançongiciel**, majoritairement perpétrée par le crime organisé, à la recherche de gains financiers. Ce type d'attaque ne cible pas spécifiquement le ministère, néanmoins le nombre d'agents susceptibles d'être atteints et l'ouverture croissante du système d'information augmentent très sensiblement la probabilité d'être touché.

D'autres menaces concernent également le ministère de la culture. Son exposition médiatique en fait ainsi une cible privilégiée de groupes activistes ou terroristes avec un **risque de défiguration des principaux sites institutionnels** et événementiels. A un niveau moindre, des organisations étatiques peuvent tenter de compromettre les ressources du ministère et, au travers du réseau interministériel, faire un rebond vers d'autres ressources plus critiques de l'Etat.

Enfin, la malveillance, avec l'utilisation par des agents de droits d'administration légitimes afin de réaliser des **actions illégitimes**, est une menace toujours d'actualité.

3.4. Stratégie de sécurisation numérique du ministère de la culture

Pour répondre à ces enjeux et faire face aux menaces qui pourraient l'impacter, le ministère fixe **cinq grandes orientations stratégiques** de la sécurité du numérique :

- **Garantir la continuité d'activité** des missions du ministère en cas d'incident de cybersécurité et renforcer le niveau de sécurité numérique afin d'atteindre un niveau de maturité adapté aux recommandations de l'Etat ;
- **Faire des agents les premiers acteurs de la sécurité**, et notamment assurer une sensibilisation continue et adaptée à leurs responsabilités et à leurs activités, afin de limiter les comportements à risques. Avec l'ouverture massive de nouveaux services numériques (télétravail, webconférence, travail collaboratif...) la sécurité ne peut plus reposer uniquement sur une gestion

centralisée de la sécurité par des spécialistes mais doit s'appuyer également sur une appropriation par les agents des risques encourus face aux menaces pesant sur le ministère.

- **Adapter le niveau de sécurité aux enjeux métiers** et aux besoins des agents. Un premier niveau d'hygiène de sécurité doit être appliqué à l'ensemble du ministère sans générer d'impact important sur les activités des agents, et éviter la mise en place de solutions de contournement. Ce niveau de sécurité doit alors être renforcé en cas d'enjeux spécifiques justifiés et validés par les responsables de la sécurité des systèmes d'information ;
- **Renforcer les relations de confiance numériques avec les tiers** (citoyens, partenaires institutionnels) et **élaborer les procédures** pour que les prestataires de services numériques respectent un niveau de sécurité approprié.
- **Mettre en place les principes de gouvernance** au sein de l'ensemble des entités rattachées au ministère en déclinaison de la réglementation de l'Etat et déployer la chaîne fonctionnelle de la sécurité du numérique.

4. Gouvernance ministérielle de la sécurité du numérique

Pour mener à bien ses missions, le ministère s'appuie sur une **chaîne fonctionnelle dédiée** et sur des **instances de gouvernance** permettant de définir la stratégie ministérielle de sécurité du numérique et d'assurer le suivi de sa mise en œuvre.

4.1. Rôles et responsabilités



4.1.1. Le ministre

Le **ministre est responsable de la sécurité numérique** des systèmes d'information et de communication du ministère et des organismes placés sous sa tutelle.

A ce titre, le ministre s'assure de la **maîtrise des risques numériques** ayant un impact sur la continuité d'activité du ministère et valide les orientations stratégiques ministérielles en matière de sécurité du numérique.

Pour l'assister, le ministre désigne un fonctionnaire de la sécurité des systèmes d'information, placé sous l'autorité du haut-fonctionnaire de défense et de sécurité.

4.1.2. Le haut-fonctionnaire de défense et de sécurité (HFDS) et par délégation le HFDS Adj

Le **haut-fonctionnaire de défense et de sécurité (HFDS)**, secrétaire général du ministère, **conseille le ministre** pour toutes les questions relatives à la sécurité de défense, la protection du secret et la sécurité du numérique.

Le HFDS est membre du comité stratégique interministériel de la sécurité du numérique et participe à l'instance stratégique ministérielle de la sécurité du numérique. Enfin, il s'assure de la prise en compte de la sécurité du numérique par les établissements publics relevant de la tutelle du ministère, en s'appuyant, notamment, sur la chaîne fonctionnelle de la sécurité des systèmes d'information du ministère.

Dans le cadre de ses missions, le **HFDS est secondé par le HFDS adjoint**, chef de service du haut-fonctionnaire de défense et de sécurité (SHFDS).

4.1.3. Le fonctionnaire de sécurité des systèmes d'information (FSSI)

Le fonctionnaire de sécurité des systèmes d'information (FSSI) définit la politique ministérielle permettant de maîtriser les risques de sécurité du numérique et de garantir la continuité des activités. Il est consulté sur la bonne prise en compte de la sécurité du numérique dans les politiques publiques du ministère et la stratégie ministérielle du numérique.

Le FSSI conseille et accompagne l'ensemble des acteurs du ministère ainsi que les établissements publics sur les questions relatives à la sécurité du numérique.

Le FSSI s'assure de la cohérence des mesures en matière de sécurité numérique et de la prise en compte, au sein du ministère et des organismes placés sous sa tutelle, du respect des règles et des orientations politiques en matière de sécurité numérique. Il contrôle l'application des exigences de sécurité définies dans le présent document à l'aide d'audits, de contrôles et de bilans.

Le FSSI pilote la réponse aux incidents majeurs de sécurité du numérique.

Le FSSI est l'interlocuteur privilégié de l'Agence nationale de sécurité des systèmes d'information (ANSSI). Il informe notamment l'ANSSI des incidents majeurs sur les systèmes d'information et de communication du ministère et des organismes placés sous sa tutelle.

Nommé par le ministre, le FSSI est placé sous l'autorité hiérarchique du haut-fonctionnaire de défense et de sécurité (HFDS).

4.1.4. L'autorité qualifiée en sécurité des systèmes d'information (AQSSI)

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est responsable de la sécurité des services numériques placés sous sa responsabilité et de leur homologation. Cependant les applications dont la maîtrise d'œuvre est assurée par le service du numérique sont homologuées par le secrétaire général du ministère.

L'AQSSI nomme, lorsqu'elle n'exerce pas elle-même cette fonction, les autorités d'homologation des systèmes d'information et de communication sous sa responsabilité.

L'AQSSI alloue les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre et s'assure à ce titre que les risques numériques sont gérés. Excepté si ces responsabilités ont été déléguées au service en charge du numérique, l'AQSSI est responsable de l'élaboration d'une cartographie de ces services et de leur maintien en condition opérationnelle et de sécurité.

L'AQSSI fournit un état annuel de la mise en œuvre de la sécurité sur son périmètre et contribue ainsi à l'élaboration du rapport annuel de sécurité qui intègre notamment l'évaluation du niveau de sécurité du numérique et une synthèse des incidents de sécurité numérique. Le rapport ministériel de sécurité est élaboré par le SHFDS s'appuyant sur les états fournis par les AQSSI et le SNUM. Ce rapport est présenté en instance stratégique ministérielle de la sécurité du numérique.

L'AQSSI participe à l'élaboration et la mise en œuvre des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité numérique. Il s'assure, notamment au travers d'exercices, de la mise à jour de ces plans.

Les AQSSI sont nommées par arrêté ministériel au titre de leur fonction. Ainsi, sont désignés « autorités qualifiées en sécurité des systèmes d'information » :

- en administration centrale, le directeur de cabinet ministériel, le secrétaire général, les directeurs généraux, les délégués généraux et l'inspecteur général des affaires culturelles ;
- en services déconcentrés, le directeur régional des affaires culturelles et directeur des affaires culturelles ;
- en établissement public, le directeur exécutif.

Les responsabilités des AQSSI sont précisées par l'arrêté portant désignation des autorités qualifiées pour la sécurité des systèmes d'information.

4.1.5. Le conseiller à la sécurité du numérique (CSN)

Le conseiller à la sécurité du numérique (CSN) conseille et accompagne l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) dans l'exercice de ses responsabilités pour la gestion des risques numériques. Il assiste notamment l'autorité qualifiée et les autorités d'homologation pour l'homologation des systèmes d'information.

Le CSN dispose d'une culture de la sécurité du numérique lui permettant d'en traduire les enjeux pour le compte de son AQSSI.

Membre du comité de direction, le conseiller à la sécurité du numérique est nommé par l'AQSSI.

4.1.6. Le chef du service du numérique (SNUM)

Le chef du service du numérique définit la stratégie ministérielle du numérique et il s'assure de la prise en compte dans son service de la politique ministérielle de sécurité du numérique.

Son service assure la mise en œuvre et l'exploitation de services numériques et d'infrastructures du ministère. Il veille, notamment dans le cadre des démarches d'homologation, à l'élaboration et au maintien à jour d'une cartographie des systèmes d'information sous sa responsabilité, à leur maintien en condition opérationnelle et de sécurité, à la réalisation d'audits de sécurité, à l'élaboration des plans de continuité et de reprise informatique et à la fourniture de moyens permettant de répondre à des crises liées à sécurité du numérique.

Le chef du service du numérique nomme un ou plusieurs responsables de la sécurité de systèmes d'information pour l'assister dans l'exercice de ses missions.

4.1.7. Le responsable de la sécurité des systèmes d'information (RSSI)

Le responsable de la sécurité des systèmes d'information (RSSI) conseille et accompagne le chef du service du numérique (SNUM), ainsi que les correspondants sécurité dans la mise en œuvre opérationnelle de la sécurité du numérique.

Le RSSI dispose d'une expertise technique en matière de sécurité du numérique. Il accompagne les démarches d'homologation, contribue à la définition de la stratégie de sécurité du numérique du ministère, contrôle opérationnellement les dispositifs de sécurisation mis en œuvre et participe à la remédiation des incidents de sécurité numérique.

Le RSSI informe le DPD et le FSSI de tout incident sur le système d'information.

Le RSSI est nommé par le chef du service du numérique.

4.1.8. Le responsable de la sécurité des systèmes d'information (DPD)

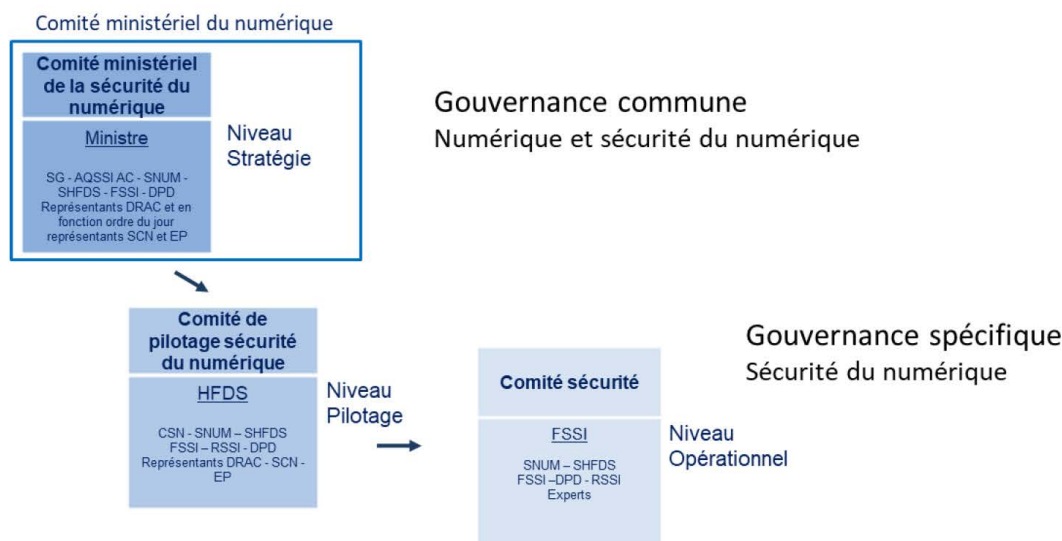
Le **délégué à la protection des données (DPD)** conseille et accompagne les services pour leur conformité au règlement général sur la protection des données (RGPD). En matière de sécurité des systèmes d'information :

- le DPD informe et conseille le SNUM sur les obligations en matière de protection des données personnelles (notamment au regard des mesures techniques et organisationnelles prévues à l'article 32 du RGPD);
- le DPD dispense des conseils concernant les analyses d'impact relatives à la protection des données (AIPD) et développe des actions de sensibilisation sur les aspects juridiques de la sécurité des données personnelles ;
- le DPD assure, en lien avec le SNUM, le RSSI et le FSSI, la notification des violations de données personnelles à l'autorité de contrôle (CNIL), dont il est l'interlocuteur privilégié, notamment pour les AIPD.

4.2. Instances ministérielles de la sécurité du numérique

Les **instances de gouvernance du numérique** permettent de traiter les enjeux de sécurité du numérique selon les **niveaux stratégique, pilotage et opérationnel**.

Dans une perspective d'efficacité, l'instance stratégique ministérielle de la sécurité du numérique pourra s'articuler avec les instances de gouvernance du numérique et celle relative à la protection des données à caractère personnel.



4.2.1. Le comité ministériel de la sécurité du numérique

Le comité ministériel de la sécurité du numérique valide les orientations stratégiques du ministère de la culture en matière de sécurité du numérique, en tenant compte des orientations prises en comité stratégique interministériel de la sécurité du numérique. Le comité ministériel de la sécurité du numérique suit également l'avancement de la feuille de route pluriannuelle déclinant cette stratégie ainsi que les indicateurs de gouvernance liés à la sécurité du numérique du ministère.

Présidée par le ministre, le comité ministériel de la sécurité du numérique est composé du haut-fonctionnaire de défense et de sécurité (HFDS) et de son adjoint, du fonctionnaire de sécurité des systèmes d'information (FSSI), du délégué à la protection des données (DPD), de l'ensemble des autorités qualifiées en sécurité des systèmes d'information de l'administration centrale (AQSSI), du chef du service du numérique (SNUM) et des représentants des directeurs régionaux des affaires culturelles (DRAC). En fonction de l'ordre du jour, cette instance peut associer toute autorité ou expert, des représentants des chefs de services à compétence nationale (SCN) et des chefs d'établissements publics sous tutelle.

Le comité ministériel de la sécurité du numérique se réunit au minimum une fois par an.

4.2.2. Le comité de pilotage sécurité du numérique

Le comité de pilotage sécurité du numérique pilote les activités relatives à la sécurité du numérique, à la continuité d'activité et à la protection des données.

Présidé par le haut-fonctionnaire de défense et de sécurité (HFDS), le comité de pilotage sécurité du numérique est composé du HFDS adjoint, du fonctionnaire de sécurité des systèmes d'information (FSSI), du chef du service du numérique (SNUM), du délégué à la protection des données (DPD), des conseillers à la sécurité du numérique (CSN) et des responsables de la sécurité des systèmes d'information du ministère (RSSI). Cette instance peut associer toute personne ou expert en fonction de l'ordre du jour.

Le comité de pilotage sécurité du numérique valide la feuille de route pluriannuelle déclinant la stratégie de la sécurité du numérique définie par l'instance stratégique ministérielle. Il assure ensuite un suivi de la mise en œuvre de cette feuille de route, des budgets et moyens qui lui sont consacrés ainsi que des indicateurs de performance et de maturité qui lui sont associés. Il suit également les chantiers majeurs liés à la sécurité du numérique, les homologations et la gestion des incidents majeurs de sécurité comportant une composante numérique.

Le secrétariat de cette instance est assuré par le fonctionnaire de sécurité des systèmes d'information (FSSI).

Le comité de pilotage sécurité du numérique se réunit au minimum une fois par an sur convocation de son président.

4.2.3. Le comité sécurité

Le comité sécurité pilote au niveau opérationnel les activités et chantiers relatifs à la sécurité du numérique, à la continuité d'activité et à la protection des données personnelles.

Le comité sécurité suit les projets et chantiers liés à la feuille de route validée par le comité de pilotage sécurité du numérique. Il valide également les règles opérationnelles de sécurité, traite les points d'arbitrage sur les orientations techniques liées à la sécurité du numérique, programme les audits, suit la mise en œuvre des plans d'action et suit les incidents majeurs de sécurité numérique. Enfin, le comité sécurité prépare les éléments en vue de la tenue des instances ministérielles de la sécurité du numérique.

Le comité sécurité est composé du chef du service du numérique (SNUM), des sous-directeurs du SNUM, du chef de service du haut-fonctionnaire de défense et de sécurité (SHFDS), du fonctionnaire de sécurité des systèmes d'information (FSSI) et des responsables de la sécurité des systèmes d'information du ministère (RSSI). Ce comité peut être élargi à toute personne ou expert en fonction de l'ordre du jour.

Animé par le FSSI, le comité se réunit au minimum une fois tous les 2 mois et autant que de nécessaire, sur proposition de ses membres.

4.3. Sécurité du numérique dans les services déconcentrés

4.3.1. Le responsable de la sécurité du numérique

Le directeur régional des affaires culturelles (DRAC) est autorité qualifiée en sécurité des systèmes d'information (AQSSI) sur son périmètre. Il est responsable de la mise en œuvre de la politique de sécurité du numérique.

L'autorité qualifiée en sécurité des systèmes d'information communique annuellement au service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère un bilan de la mise en œuvre de la sécurité du numérique dans son entité.

Par ailleurs, il est l'interlocuteur du service du haut fonctionnaire de défense et de sécurité (SHFDS) dans le cadre d'une crise cybersécurité.

Pour l'assister, l'autorité qualifiée en sécurité des systèmes d'information s'appuie sur un conseiller sécurité du numérique - membre du comité de direction -, et sur un correspondant sécurité du numérique.

4.3.2. Le correspondant sécurité du numérique

Le responsable informatique de la direction régionale aux affaires culturelles est correspondant sécurité du numérique, soutien opérationnel de son directeur sur la sécurité du numérique.

Le correspondant sécurité du numérique est l'interlocuteur privilégié du service du numérique (SNUM) et du service du haut fonctionnaire de défense et de sécurité (SHFDS) sur tous les sujets opérationnels relatifs à la sécurité du numérique.

4.4. Sécurité dans les services à compétence nationale (SCN)

4.4.1. Le responsable de la sécurité du numérique

Le directeur du service à compétence nationale est responsable, sur son périmètre, de la mise en œuvre de la politique de sécurité du numérique.

Le directeur du service à compétence nationale communique annuellement à son autorité qualifiée en sécurité des systèmes d'information (directeur général ou délégué général) et au service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère, un bilan de la mise en œuvre de la sécurité du numérique dans son service.

Par ailleurs, il est l'interlocuteur du service du haut fonctionnaire de défense et de sécurité (SHFDS) dans le cadre d'une crise cybersécurité.

Pour l'assister, le directeur du service à compétence nationale d'information s'appuie sur un correspondant sécurité du numérique.

Avec l'accord de leur autorité qualifiée en sécurité des systèmes d'information, les directeurs des grands services à compétence nationale pourront nommer un **conseiller à la sécurité du numérique**, membre du comité de direction.

4.4.2. Le correspondant sécurité du numérique

Le correspondant informatique du service à compétence nationale (SCN) est correspondant sécurité du numérique, soutien opérationnel de son directeur sur la sécurité du numérique.

Le correspondant sécurité du numérique est l'interlocuteur privilégié du service du numérique (SNUM) et du service du haut fonctionnaire de défense et de sécurité (SHFDS) sur tous les sujets opérationnels relatifs à la sécurité du numérique.

4.5. Gouvernance sécurité dans les établissements publics

Afin de se mettre en conformité avec la loi et être plus résilient face aux attaques, les **établissements publics sous tutelle du ministère doivent décliner la politique ministérielle de sécurité du numérique** et mettre en place une organisation et des moyens permettant de garantir la sécurité de leurs services numériques et la continuité d'activité.

4.5.1. Le responsable de la sécurité du numérique

Le dirigeant exécutif de l'établissement est responsable, sur son périmètre, de la sécurité du numérique et de la continuité d'activité.

Le dirigeant exécutif de l'établissement est autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) de son établissement. Il peut désigner un **conseiller à la sécurité numérique**, membre du comité de direction, pour piloter les activités relatives à la sécurité du numérique, à la continuité d'activité et à la protection des données personnelles.

4.5.2. L'organisation de la gouvernance

Le dirigeant exécutif de l'établissement **décline la politique ministérielle de sécurité du numérique (PSNum)**. Il s'assure notamment de la définition et de la mise en œuvre d'une organisation adaptée aux enjeux et aux moyens de son établissement pour garantir la sécurité des services numériques.

En l'absence de déclinaison de la PSNum, la politique ministérielle s'applique.

4.5.3. Le point de contact relatif à la sécurité du numérique

Le dirigeant exécutif de l'établissement nomme sous sa responsabilité directe un **soutien opérationnel** pour garantir la sécurité de ses services numériques.

En fonction des enjeux de sécurité et des moyens de son établissement, le dirigeant exécutif peut soit nommer un responsable de la sécurité des systèmes d'information (RSSI) dédié, soit attribuer cette mission au chef des services informatiques de l'établissement.

Ce point de contact est l'interlocuteur privilégié du ministère de la culture et de l'Agence nationale de la sécurité des systèmes d'information sur tous les sujets opérationnels relatifs à la sécurité du numérique.

4.5.4. Mise en œuvre de la politique sécurité du numérique

Le dirigeant exécutif de l'établissement consolide et communique annuellement au service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère un **bilan de la mise en œuvre de la sécurité du numérique** de son établissement.

Le haut fonctionnaire de défense et de sécurité (HFDS) peut en complément demander au dirigeant exécutif de **conduire un état des lieux ou un audit** sur un périmètre particulier.

4.5.5. La déclaration des incidents de sécurité

Le dirigeant exécutif de l'établissement doit **informer le SFDHS des incidents majeurs de sécurité du numérique**. Le SHFDS pourra alors apporter son soutien pour la coordination des actions de remédiation et obtenir l'appui des experts du ministère et des instances gouvernementales.

4.6. Relation entre le ministère et les autorités administratives

Le haut-fonctionnaire de défense et de sécurité (HFDS) est l'interlocuteur privilégié du directeur général de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** sur les sujets relatifs à la sécurité du numérique de niveau stratégique.

Le fonctionnaire de sécurité des systèmes d'information (FSSI) est un interlocuteur privilégié de l'ANSSI sur les sujets d'élaboration et de mise en œuvre de la sécurité du numérique au sein du ministère et sur ceux liés au suivi de la **feuille de route ministérielle de sécurité du numérique**.

En tant que pilote de la chaîne fonctionnelle de la sécurité des systèmes d'information, le FSSI notifie dans les plus brefs délais les incidents de sécurité significatifs à l'ANSSI. Il informe le **délégué à la protection des données ministériel (DPD)**, notamment si des données à caractère personnel sont susceptibles d'être concernées.

Enfin, le FSSI apporte un soutien au DPD ministériel dans le cadre des **relations avec la commission nationale de l'informatique et des libertés (Cnil)** sur les sujets liés à la sécurité des données à caractère personnel.

5. Règles et processus de sécurité du numérique



Les règles sécurité

Les processus sécurité		
Identifier et cartographier	Protéger et planifier	Détecter et répondre
<ul style="list-style-type: none">La cartographie des infrastructures, des applications et des donnéesLa classification des données par niveau de sensibilitéLa cartographie des risques	<ul style="list-style-type: none">L'intégration de la sécurité dans les projets (applicatifs et d'infrastructure) et les prestationsL'homologationLe maintien en conditions de sécurité des infrastructures et des applicationsLa protection des données personnellesLa sensibilisation et la formation à la sécuritéLa continuité d'activitéLa gestion des dérogations	<ul style="list-style-type: none">La veille sécurité des systèmes d'informationLa supervision continue des infrastructures et des applicationsLa gestion des alertes et des incidentsLa gestion de crise cybersécuritéLes contrôles

5.1. Règles de sécurité

Le référentiel des règles de sécurité du ministère s'appuie sur la politique de sécurité des systèmes d'information de l'Etat (PSSI-E) de 2014. Le ministère s'appuiera sur le nouveau référentiel ministériel de règles de sécurité dès sa publication, après déclinaison au contexte spécifique du ministère.

La directive « règles de sécurité du numérique » précisera les principales règles de sécurité prioritaires pour le ministère.

Tous les agents du ministère doivent respecter ces règles de sécurité, suivre les recommandations définies en application de celles-ci et utiliser les infrastructures et les outils mis à leur disposition dans les conditions d'usage précisées.

Les autorités qualifiées pour la sécurité des systèmes d'informations (AQSSI) s'assurent de la mise en œuvre des règles de sécurité sur leur périmètre de responsabilité et du respect des exigences réglementaires.

5.2. Principaux processus de sécurité

Identifier et cartographier

5.2.1. La cartographie des infrastructures, des applications et des données

La **cartographie** des infrastructures, des applications et des données du ministère permet d'**identifier l'ensemble des actifs du système d'information**. Cet inventaire documenté et à jour permet notamment de déterminer les périmètres nécessitant une homologation et de faciliter une réaction rapide et adaptée en cas d'incident ou de crise cybersécurité.

Chaque actif du ministère (infrastructures, applications ou données) est placé sous la responsabilité d'un référent.

Les autorités qualifiées pour la sécurité des systèmes d'information (AQSSI), et le service du numérique par délégation, doivent, sur leur périmètre, cartographier les actifs et identifier leurs responsables.

5.2.2. La classification des données par niveau de sensibilité

Pour protéger son patrimoine culturel numérique et respecter la réglementation, notamment celle concernant la protection des données sensibles, le ministère a élaboré une **échelle de classification des données par niveau de confidentialité**. Le ministère doit ensuite identifier les données et préciser les consignes pour garantir la confidentialité et la protection de ces données.

Le niveau de sécurité des données du ministère est évalué sur une échelle de 4 niveaux : les **données publiques (DP)**, les **données internes (C1)**, les **données sensibles internes (C2)** et les **données classifiées** selon l'Instruction Générale Interministérielle 1300 (C3).

Mention	Libellé	Description
C3	Données classifiées	Classification réservée aux rares informations dont la divulgation pourrait porter atteinte aux intérêts stratégiques, à la sécurité ou à l'existence du Ministère et de l'Etat <ul style="list-style-type: none">Données régies par l'IG1300 Ces données sont gérées sur des infrastructures spécifiques interministérielles et ne sont accessibles qu'aux personnes habilitées « Secret » et « Très Secret »
C2	Données internes sensibles	Pour les informations relevant d'une protection particulière <ul style="list-style-type: none">Echanges entre les hautes autorités : conseillers, ministres, sécurité...Données d'administration et d'exploitation informatiqueDocuments portant la mention Diffusion Restreinte (DR)

		<ul style="list-style-type: none"> Données sensibles au sens RGPD (biométriques, de santé...)
C1	Données internes	<p>Données internes au ministère accessibles par les personnes identifiées et autorisées à l'intérieur du Ministère.</p> <ul style="list-style-type: none"> Notes, projets, dossiers..., Données personnelles non sensibles
DP	Données publiques	<p>Informations pouvant circuler librement à l'extérieur de notre périmètre</p> <ul style="list-style-type: none"> Données publiées sur internet, en accès libre par le public, sur le site data.gouv.fr...

Les autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) évaluent, sur leur périmètre de responsabilité, le niveau de sensibilité de leurs données selon cette échelle et précisent par note les procédures à mettre en œuvre pour garantir la confidentialité de ces données.

Par ailleurs, les documents produits ou échangés au sein du ministère doivent faire apparaître de manière explicite leur niveau de confidentialité

5.2.3. La cartographie des risques

L'identification et la classification des risques de sécurité numérique permet de déterminer et de prioriser les axes d'amélioration pour mieux protéger le patrimoine informationnel et matériel et de garantir la continuité d'activité.

Le fonctionnaire à la sécurité des systèmes d'information (FSSI) réalise la cartographie des risques et l'élaboration d'un plan pluriannuel de traitement des risques numériques prioritaires, avec l'aide des responsables de la sécurité des systèmes d'information (RSSI), des équipes du service du numérique (SNUM) et des conseillers à la sécurité du numérique (CSN).

Protéger et planifier

5.2.4. L'intégration de la sécurité dans les projets et les prestations

L'intégration de la sécurité dans les projets applicatifs et d'infrastructure numérique doit se faire tout au long de leur cycle de vie, de la conception au fonctionnement en production, afin de réduire les risques numériques et de diminuer les coûts.

Les exigences de sécurité doivent être spécifiées dans les cahiers des charges d'appel d'offre en s'appuyant sur les clauses contractuelles élaborées par la direction des Achats de l'Etat (DAE) et par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

La démarche d'intégration de la sécurité dans les projets et dans les prestations est élaborée par le service du numérique en coordination avec le fonctionnaire à la sécurité des systèmes d'information (FSSI). Elle est ensuite mise en œuvre par les équipes projet des directions métiers et les équipes du service du numérique (SNUM). Au sein du ministère, cette

démarche est notamment cadrée à l'aide d'un « diagnostic éclair » réalisé au début de tout projet, qu'il soit réalisé ou non selon la méthode Agile.

5.2.5. L'homologation

L'homologation de sécurité, qui est un préalable indispensable à l'instauration de la **confiance dans les services numériques**, est une décision formelle, prise par l'autorité d'homologation, par laquelle il atteste de sa connaissance des risques numériques ainsi que des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre pour supprimer ces risques ou les rendre acceptables.

L'homologation est rendue obligatoire par l'instruction générale interministérielle 1300 et par le référentiel général de sécurité (RGS). A ce titre, doivent être homologués, tous les systèmes d'information relatifs aux échanges électroniques entre les usagers et les autorités administratives, ceux relatifs aux échanges entre les autorités administratives, ainsi que toutes les infrastructures majeures utilisées par ces services.

Le service du numérique (SNUM) identifie et planifie, avec les directions métier, l'ensemble des services numériques et infrastructures devant faire l'objet d'une homologation. Le **plan pluriannuel d'homologation** est validé en comité de pilotage sécurité du numérique.

Le « diagnostic éclair » permet de déterminer si un service ou une infrastructure numérique doit faire l'objet d'une homologation et quels sont les travaux nécessaires pour construire le dossier d'homologation (analyse de risque, audit de sécurité pouvant comprendre des revues d'architecture ou de configuration ainsi que des tests d'intrusion, formalisation du dossier d'architecture et des procédures de maintien en conditions de sécurité).

La **décision d'homologation** est prise dans le cadre d'une commission dédiée et fixe une durée d'homologation, ne pouvant dépasser 3 ans, en fonction de la criticité du périmètre étudié.

Si l'autorité d'homologation considère que les conditions ne sont pas réunies pour une homologation et que le refus d'homologation n'est pas envisageable, **une autorisation provisoire d'emploi** peut être prononcée pour une durée courte (3 ou 6 mois). Elle est assortie de conditions strictes et d'un plan d'action précis, destiné à maîtriser les risques encore trop élevés durant ce laps de temps.

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est, par défaut, l'autorité d'homologation des services numériques et d'infrastructures de son périmètre de responsabilité. Cependant les applications dont la maîtrise d'œuvre est assurée par le service du numérique sont homologuées par le secrétaire général du ministère qui est également l'autorité d'homologation des projets d'infrastructures portés par le SNUM.

Un directeur général peut cependant désigner autorité d'homologation le directeur d'un service à compétence nationale (SCN) dont il a la tutelle pour les périmètres lui étant spécifiques.

La commission d'homologation est présidée par l'AQSSI ou par son mandataire. Le fonctionnaire à la sécurité des systèmes d'information (FSSI) participe aux commissions d'homologation et donne un avis formel. En cas de divergence entre l'autorité d'homologation et le FSSI, le haut fonctionnaire de défense et de sécurité (HFDS) prend ou non la décision d'homologuer un service ou une infrastructure.

5.2.6. Le maintien en conditions de sécurité des infrastructures et des applications

Le **maintien en conditions de sécurité (MCS)** permet de garder les services et les infrastructures numériques à un niveau de sécurité qui **garantit leur fonctionnement et l'intégrité des données**.

Le maintien en conditions de sécurité comprend le durcissement de la configuration des ressources déployées, l'application, éventuellement en urgence, des correctifs publiés par les éditeurs et fournisseurs afin de traiter les vulnérabilités, la mise à jour des dispositifs de sécurité comme les antivirus et enfin l'anticipation sur l'obsolescence des ressources utilisées.

Les procédures de maintien en conditions de sécurité sont définies par les responsables de la sécurité des systèmes d'information (RSSI) et validées par le comité de sécurité du numérique. Ces procédures sont ensuite appliquées par les équipes du service du numérique (SNUM), par les responsables informatiques des directions régionales aux affaires culturelles (DRAC) et par les correspondants informatiques des services à compétence nationale (SCN).

En cas de défaut du maintien en conditions de sécurité d'un service, l'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) ou le fonctionnaire à la sécurité des systèmes d'information (FSSI) pourront demander l'arrêt des ressources concernées jusqu'à la correction des failles. En dernier recours, c'est le haut fonctionnaire de défense est de sécurité (HFDS) qui pourra prendre cette décision pour toute ressource du ministère.

5.2.7. La protection des données personnelles

Le **règlement général sur la protection des données personnelles** du 27 avril 2016 (RGPD) responsabilise les organismes publics et privés traitant de données personnelles, c'est-à-dire de toute information se rapportant à une personne physique identifiée ou identifiable.

Conformément à l'article 32 du RGPD, le ministère doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de **garantir la sécurité des données personnelles**. En cas de risque identifié sur un traitement par le délégué à la protection des données (DPD), une analyse d'impact relative à la protection des données (AIPD) est conduite avec son concours.

La **stratégie de sécurité des services numériques liée à la protection des données personnelles** est définie par le délégué à la protection des données (DPD) et par le fonctionnaire à la sécurité des systèmes d'information (FSSI), avec le soutien des responsables de la sécurité des systèmes d'information (RSSI).

5.2.8. La sensibilisation et la formation à la sécurité

Pour **faire des agents les premiers acteurs de la sécurité**, le ministère définit et met en œuvre un plan de sensibilisation et de formation pluriannuel à la sécurité du numérique pour l'ensemble de ses agents :

- des formations à la sécurité pour les **équipes du service du numérique (SNUM)** afin qu'ils consolident les connaissances nécessaires à la réalisation de leurs tâches ;
- des sensibilisations spécifiques pour l'**encadrement supérieur** du ministère qui a un rôle d'ambassadeur de la sécurité numérique auprès des agents ;

- des communications et des formations pour l'ensemble des agents du ministère pour les préparer à faire face aux principaux vecteurs d'attaque les visant, comme des exercices d'hameçonnage.

Le plan de sensibilisation et de formation, qui est piloté par le fonctionnaire à la sécurité des systèmes d'information (FSSI), est validé en comité de pilotage sécurité du numérique.

5.2.9. La continuité d'activité

Le plan de continuité d'activité permet, lors d'un sinistre majeur, de poursuivre les activités essentielles du ministère.

Le ministère doit identifier les menaces potentielles, ainsi que les impacts que ces menaces peuvent avoir sur ses activités. Il doit également élaborer un plan pour augmenter la résilience de son système d'information avec pour objectif la préservation des intérêts et de la réputation du ministère. Ainsi :

- le service du haut fonctionnaire de défense et de sécurité (SHFDS) et le fonctionnaire à la sécurité des systèmes d'information (FSSI) définissent la stratégie permettant de garantir la continuité des activités du ministère face aux risques de sécurité du numérique et en pilotent la mise en œuvre ;
- Les autorités qualifiées de la sécurité des systèmes d'information (AQSSI) s'assurent, avec le soutien du SHFDS, de l'élaboration, de la mise en œuvre et du maintien, notamment au travers d'exercices, des plans de continuité et de reprise des activités relevant de leur domaine de responsabilité ;
- Enfin, le chef du service du numérique (SNUM) est responsable de l'élaboration, de la mise en œuvre et du maintien du volet numérique des plans de continuité et de reprise d'activité.

5.2.10. La gestion des dérogations

Toute demande de dérogation aux règles et aux référentiels de sécurité en vigueur doit être formalisée et motivée. La demande de dérogation est ensuite examinée au regard des directives ou règles sur lesquelles elle porte, des besoins la justifiant et des risques que son approbation induit pour le ministère. La décision doit être justifiée et tracée, et une dérogation ne doit être valable que pour une durée déterminée.

Le chef du service du numérique (SNUM) est responsable de l'approbation de toute demande de dérogation liée aux prestations et aux infrastructures fournies par son service. Il s'appuie sur les responsables de la sécurité des systèmes d'information (RSSI) pour répondre aux demandes et les valider.

Le fonctionnaire à la sécurité des systèmes d'information (FSSI) est chargé de valider les autres demandes de dérogations, en particulier celles concernant les dérogations aux règles de la présente politique de sécurité du numérique, celles concernant l'utilisation de ressources numériques non supportées par le SNUM et celles concernant les principes définis dans le cadre d'une homologation.

En dernier recours le haut fonctionnaire de défense et de sécurité (HFDS) valide ou non la dérogation.

Détecter et répondre

5.2.11. La veille sécurité des systèmes d'information

La **veille sécurité des systèmes d'information** permet d'anticiper, de détecter et de corriger les vulnérabilités de sécurité numérique qui pourraient impacter le ministère.

Le ministère doit consulter les publications des nouvelles vulnérabilités par les éditeurs, les bulletins d'actualités présentant les mesures de sécurité à appliquer et être abonné aux publications d'un ou plusieurs CERT (Computer Emergency Response Team). Ces publications feront l'objet d'alertes si elles concernent des infrastructures numériques du ministère.

Les responsables de sécurité des systèmes d'informations (RSSI) mettent en place et suivent des dispositifs de veille sécurité des systèmes d'information et communiquent les informations pertinentes recueillies lors de cette veille aux responsables des différents actifs (infrastructures, applications...).

5.2.12. La supervision continue des infrastructures et des applications

La **supervision continue des services et infrastructures numériques** permet de détecter les alertes, d'identifier les dysfonctionnements et les incidents de sécurité. La supervision recouvre les scans de vulnérabilité, l'analyse des flux réseau et des flux applicatifs, la détection de signaux faibles, la gestion et la corrélation de traces.

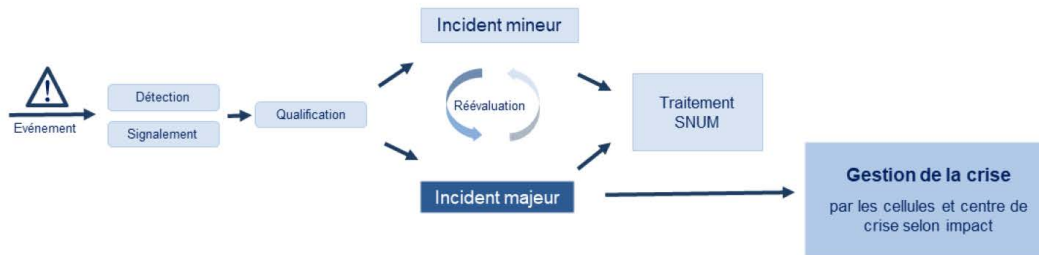
Le service du numérique (SNUM) est responsable de la spécification, de la mise en œuvre et du pilotage des services permettant la supervision continue des infrastructures et des services numériques.

Lorsque cela est nécessaire, le ministère fait appel à des expertises externes pour la supervision de ses infrastructures et ses applications. Il s'appuie également sur les services de supervision interministériels de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et du réseau interministériel de l'état (RIE).

5.2.13. La gestion des alertes et des incidents

La **gestion des alertes et des incidents** permet de qualifier et de traiter tout événement qui **porte atteinte à la disponibilité, la confidentialité ou l'intégrité** d'une ressource du ministère, afin de réduire son impact.

Le ministère doit qualifier les incidents de sécurité par niveau de gravité (**mineur, majeur**). Un **incident est dit majeur** lorsque l'impact ne permet plus au service du numérique (SNUM) de respecter ses engagements de service, ou conduit à une dégradation forte des conditions de travail des agents du ministère, et lorsque le ministère est victime d'une intrusion dans le système d'information.



Les équipes du SNUM chargées de la supervision des ressources numériques consignent et qualifient les alertes de sécurité :

- **pour un incident mineur**, les équipes du SNUM sont chargées de sa résolution et se coordonnent avec les responsables de la sécurité des systèmes d'information (RSSI), qui leur apportent un support lorsque des expertises particulières sont nécessaires ;
- **pour un incident majeur**, le chef du SNUM et le FSSI sont informés. Les RSSI sont responsables de la résolution de l'incident avec le support des équipes du SNUM. Sur proposition du FSSI, le haut fonctionnaire de défense et de sécurité adjoint (HFDS Adj) active la **cellule de crise Cybersécurité** en cas d'impact important.

Après résolution, tout incident fait l'objet d'un retour d'expérience : évaluation des origines, des impacts et de son traitement, et peut être suivi d'un plan d'actions pour en supprimer ou maîtriser les causes.

Les services du ministère devront s'appuyer sur un CERT (Computer Emergency Response Team) pour l'identification et la remédiation des incidents de cybersécurité.

5.2.14. La gestion de crise cybersécurité

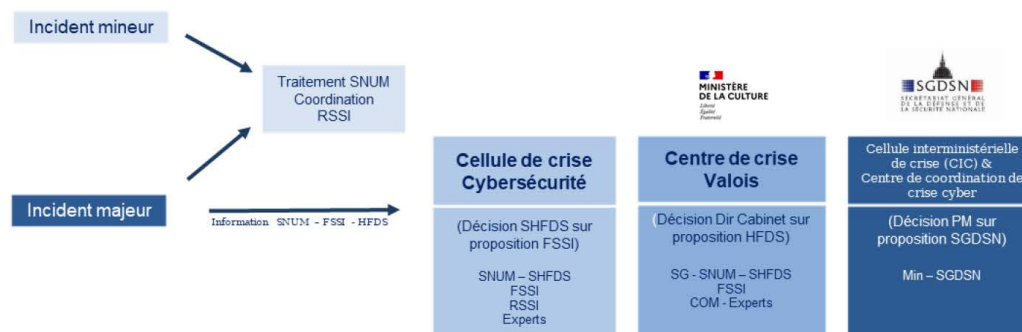
Une crise cybersécurité est un événement provoquant une déstabilisation majeure du ministère, pouvant engendrer parfois des dégâts irréversibles. Elle peut faire suite à un accident (incendie, inondation...), à des actions malveillantes comme une attaque informatique ou à une rupture des fluides (électricité, réseaux) nécessaires au bon fonctionnement des services du numérique.

Le ministère doit prendre en compte la sécurité du numérique dans le dispositif ministériel de gestion de crise. Il doit ainsi déterminer les typologies d'événements remettant en cause la disponibilité, l'intégrité ou la confidentialité de ses ressources numériques et susceptibles de générer une crise ainsi que le dispositif d'escalade permettant de décider le passage en situation de crise cybersécurité.

Trois niveaux d'escalade successifs sont définis, en fonction de la criticité du ou des services numériques affectés et de la gravité des conséquences de l'événement.

- une crise de premier niveau est traitée par la **cellule de crise cybersécurité** du ministère ;
- en cas de crise majeure, le **centre de crise Valois** est activé par le Cabinet sur proposition du HFDS ;

- enfin, en cas de crise majeure concernant plusieurs entités ministérielles, le **centre interministériel de coordination de crise cyber** est activé sur décision du Premier ministre.



La **cellule de crise cybersécurité** définit la stratégie de réponse à la crise, coordonne les actions et prépare la communication interne et externe. En préparation de crises majeures, le SHFDS s'assure de l'articulation du dispositif de crise ministériel avec le dispositif de gestion des crises majeures de cybersécurité de l'État et de l'Agence nationale de la sécurité des systèmes d'information

La cellule de crise cybersécurité est pilotée par le FSSI. Elle est composée du chef de service du numérique (SNUM) et des responsables de la sécurité des systèmes d'information (RSSI) et peut être élargie à toute personne pertinente pour traiter la crise, comme le délégué à la protection des données (DPD) ou le service en charge de la communication du ministère.

Les dispositifs de crise cybersécurité doivent être testés régulièrement au travers d'exercices ministériels ou interministériels afin de garantir leur efficacité en cas de situation réelle. Le fonctionnaire de sécurité des systèmes d'information (FSSI) participe à l'organisation des **exercices de gestion de crise cybersécurité** interministérielle.

A l'instar des autres situations de crise, la gestion de crise cybersécurité fait l'objet de **retours d'expérience** permettant d'adapter la doctrine et les pratiques dans un processus constant d'amélioration.

5.2.15. Les contrôles

Les **contrôles** permettent de vérifier que la **politique de sécurité du numérique est correctement respectée**. Ces contrôles peuvent être réalisés par évaluation du niveau de sécurité, par bilan des actions réalisées et par des audits.

Le ministère définit chaque année un **plan précisant les contrôles** à réaliser. Ce plan contient au minimum un état des lieux de la conformité du ministère à sa politique de sécurité du numérique ainsi qu'un bilan des travaux de sécurisation mis en œuvre lors des 12 derniers mois. Les écarts identifiés suite aux contrôles sont étudiés et font l'objet d'un plan de remédiation.

Au niveau opérationnel, des contrôles de sécurité sont définis et intégrés directement dans les procédures existantes.

Le plan annuel de contrôle de la sécurité du numérique est défini par le fonctionnaire de la sécurité des systèmes d'information (FSSI) avec le support des responsables de la sécurité des systèmes d'information (RSSI). Le FSSI et les RSSI en suivent alors l'application et déterminent les plans de remédiation à l'issue des contrôles.

Les autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) du ministère et des établissements publics remettent annuellement au haut-fonctionnaire de défense et de sécurité (HFDS) un bilan annuel de la mise en œuvre de la sécurité du numérique dans leur établissement.

5.3. Corpus documentaire de la politique sécurité

Ce document maitre de la politique sécurité du numérique (PSNum) qui décrit les principes de gouvernance de la sécurité du numérique au sein du ministère, sera décliné en chartes et directives opérationnelles. Elles préciseront notamment :

- les règles professionnelles et de déontologie applicables aux agents du ministère dans le cadre de l'utilisation des services numériques ;
- les règles spécifiques pour les exploitants ;
- les règles pour le développement des services numériques ;
- les processus liés à la gestion de la sécurité (gestion des incidents de sécurité numérique, gestion de crise numérique, gestion des dérogations...).

6. Principales références

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) ;
- le code de la défense, notamment ses articles L. 2321-1 et R. 1143-1 à R. 1143-8 ;
- le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;
- le 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.
- l'instruction interministérielle n° 920 /SGDSN/ DCSSI du 12 janvier 2005 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel défense (Secret) ;
- la circulaire n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'Etat (PSSIE) ;
- l'instruction interministérielle n° 901 SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles (DR) ;
- l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale ;
- Le référentiel général de sécurité (RGS) du 13 juin 2014 pris en application 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.

7. Glossaire

ANSSI (Agence nationale de sécurité des systèmes d'information) : l'ANSSI définit la stratégie de la sécurité du numérique de l'état. Elle a également chargée de missions de défense des systèmes d'information de conseil et de soutien aux administrations et aux opérateurs.

AQSSI (Autorité qualifiée en sécurité des systèmes d'information) : l'AQSSI est responsable de la sécurité numérique des services numériques placés sous sa responsabilité et de leur homologation.

Autorité d'homologation : personne physique qui prononce la décision d'homologation de sécurité d'un système d'information, et prend ainsi la décision d'accepter les risques résiduels.

Crise : une crise cybersécurité se définit par ses impacts, notamment sur les services numériques (ex : indisponibilité suite à un rançongiciel), dont les conséquences sont perceptibles au niveau métier (ex : interruption ou perturbation de l'activité, conséquences financières, juridiques ou en termes d'image).

CSN (Conseiller à la sécurité du numérique) : le CSN conseille et accompagne l'autorité qualifiée en sécurité des systèmes d'information dans l'exercice de ses responsabilités pour la gestion des risques numériques.

FSSI (Fonctionnaire de sécurité des systèmes d'information) : le FSSI définit la politique ministérielle permettant de maîtriser les risques de sécurité du numérique et de garantir la continuité des activités. Il s'assure de la mise en œuvre de la sécurité du numérique dans le ministère et dans les établissements publics sous tutelle.

HFDS (Haut-fonctionnaire de défense et de sécurité) : le HFDS conseille le ministre pour toutes les questions relatives à la sécurité de défense et de protection du secret.

Résilience numérique : la résilience numérique désigne la capacité d'une organisation à mettre en place les moyens opérationnels adaptés aux menaces et à les déployer pour, en cas de crise, être en mesure de maintenir et rétablir les services rendus par les systèmes d'information.

RSSI (Responsable de la sécurité des systèmes d'information) : le RSSI conseille et accompagne le chef du service du numérique dans la mise en œuvre opérationnelle de la sécurité du numérique. Chaque responsable d'établissement public désigne un RSSI.

Sécurité du numérique : ensemble des activités organisationnelles, techniques ou juridiques visant à protéger les services numériques, ainsi que les informations qu'ils manipulent, des incidents de sécurité de nature accidentelle ou intentionnelle.

Service numérique : prestation informatique qui s'appuie sur un ou plusieurs systèmes d'information.

Système d'information : ensemble des moyens informatiques (matériels et logiciels) mis en œuvre pour opérer un service numérique (bureautiques, applications, systèmes opérationnels)

8. Annexes

8.1. Missions des autorités qualifiées pour la sécurité des systèmes d'information (AQSSI)

Selon l'arrêté portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministère de la culture.

L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) est responsable de la sécurité du numérique au sein de sa direction ou de son établissement.

En liaison avec le haut fonctionnaire de défense et de sécurité (HFDS) et le fonctionnaire de sécurité des systèmes d'information (FSSI), l'autorité qualifiée est notamment chargée :

- d'allouer les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre et de s'assurer que les risques numériques sont gérés ;
- d'homologuer les systèmes d'information placés sous sa responsabilité et relevant du référentiel général de sécurité ;
- de s'assurer que les dispositions réglementaires sur la sécurité des systèmes d'informations traitant des données sensibles et classifiées sont appliquées ;
- de faire appliquer la politique sécurité du numérique du ministère et les directives internes ;
- de s'assurer que des contrôles internes de sécurité sont régulièrement effectués ;
- d'organiser la sensibilisation et la formation du personnel aux questions de sécurité ;
- d'élaborer et de mettre en œuvre des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité numérique.