GOUVERNEMENT
Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Politique de sécurité numérique

Version	1.0
Approuvée par la directrice interministérielle du numérique	Date : 26 juillet 2024 Signature : 

Table des matières

Préambule

Le présent document définit la politique de sécurité numérique de la direction interministérielle du numérique (PSN-DINUM).

Cette politique s'inscrit dans le cadre de la politique de sécurité des systèmes d'information de l'État (PSSI-E), approuvée par la circulaire du Premier ministre n°5725/SG du 17 juillet 2014. Elle expose les principes stratégiques structurant l'action de la DINUM en matière de sécurité numérique et précise l'organisation et la gouvernance en place, en conformité avec l'instruction générale interministérielle 1337[1]. A ce titre, elle présente les dispositions générales permettant d'assurer la protection et la défense des systèmes d'information.

Dans la suite du document, le terme « produit » est utilisé de manière générique pour désigner tous les systèmes d'information de la DINUM.

Article 1. Champ d'application

La PSN-DINUM s'applique à l'ensemble des personnels et des systèmes d'information (SI) de la DINUM.

La PSN-DINUM s'applique également, par voie contractuelle ou conventionnelle, aux services externalisés par la DINUM (fournisseurs, prestataires de services, sous-traitants…) ainsi qu'aux partenaires (ministères…) lorsqu'ils concourent aux missions de la DINUM ou qu'ils ont accès à des informations sensibles dont elle est propriétaire ou gestionnaire. L'ensemble de ces acteurs proches est appelé « écosystème numérique » de la DINUM.

Pour les échanges d'informations classifiées de défense, il appartient à l'autorité qualifiée, en lien avec l'officier de sécurité, d'appliquer la réglementation spécifique (IGI 1300[2]).

Article 2. Caractère obligatoire de la PSN-DINUM

Déclinaison de la PSSI des SPM publiée par note du 1er décembre 2022, la PSN-DINUM constitue le cadre obligatoire dans lequel tout système d'information entrant dans le champ d'application de l'article 1, doit mettre en œuvre les actions liées à la sécurité numérique.

Article 3. Révision et dérogation

La mise en œuvre de la PSN-DINUM est suivie annuellement lors d'un comité de direction[3] dédié aux aspects de sécurité numérique.

Toute demande d'évolution ou d'adaptation de la PSN-DINUM est soumise pour approbation à l'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI). A ce titre, toute dérogation à l'une des exigences de la PSSI des SPM doit être formellement autorisée par le haut fonctionnaire de défense et de sécurité des services du Premier ministre (SPM).

La PSN-DINUM est révisée en tant que de besoin et au plus tard tous les trois ans.

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046503128
[2] https://www.sgdsn.gouv.fr/missions/proteger-le-secret-de-la-defense-nationale/
[3] Voir article 16

Article 4. Corpus de la sécurité numérique

La PSN-DINUM est complétée par un corpus documentaire mis à disposition de tous les agents de la DINUM sur le service RESANA.

Ce corpus précise la manière dont les principes sont mis en œuvre de manière opérationnelle. Il indique également comment les règles de la PSSI-E sont adaptées au contexte de la DINUM.

Pour chaque document constitutif du corpus de la sécurité numérique, un porteur est désigné pour son élaboration et son maintien à jour.

Pour le compte de l'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI), le conseiller à la sécurité numérique (CSN) assure la maîtrise et le contrôle des documents publiés, relevant d'un caractère normatif pour la DINUM. Il maintient à jour la liste structurée des documents, de leur publication et de leurs mises à jour.

TITRE I : Organisation interne de la sécurité numérique

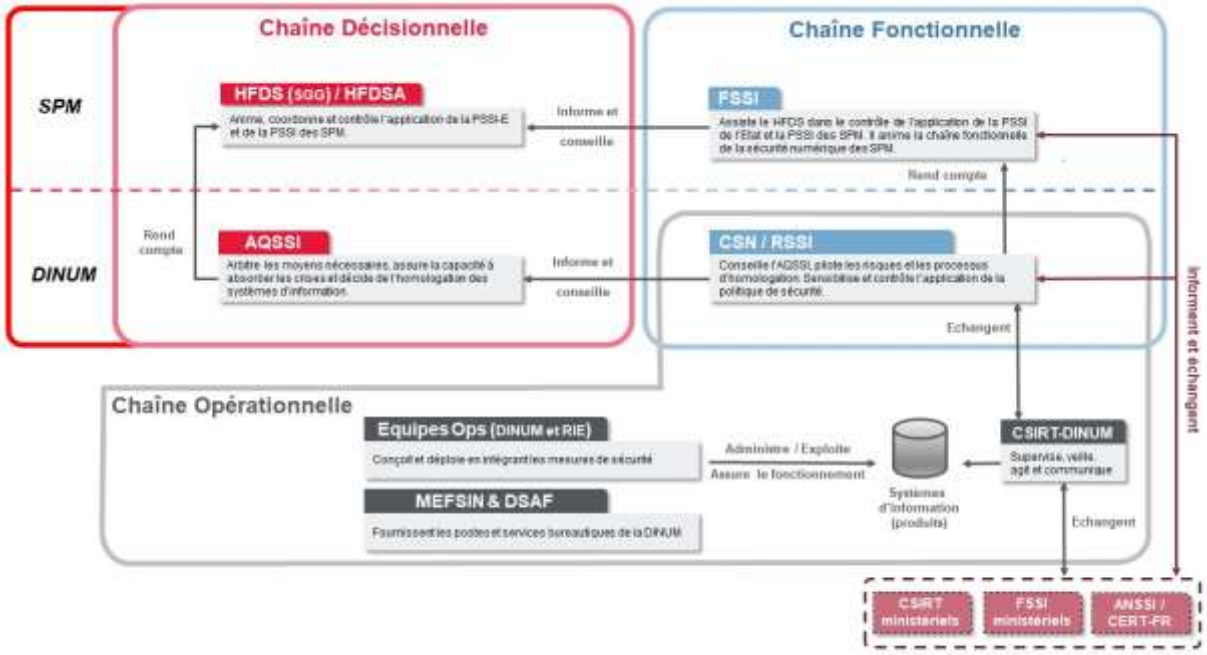

Figure 1 : Organisation générale de la sécurité numérique

Article 5. Le haut fonctionnaire de défense et de sécurité

Conformément aux missions édictées par l'article R1143-5 du Code de la Défense et l'IGI 1300, le haut fonctionnaire de défense et de sécurité (HFDS) anime la politique de sécurité et contrôle son application. Pour les SPM, le secrétaire général du gouvernement (SGG) est désigné HFDS.

En vue de garantir la sécurité globale des SPM, le HFDS anime, coordonne et contrôle l'application de la PSSI-E et de la PSSI des SPM par les autorités qualifiées en sécurité des systèmes d'information.

Pour exercer ses missions, il s'appuie sur le haut fonctionnaire de défense et de sécurité adjoint (HFDSa), chef du service du HFDS.

Article 6. L'autorité qualifiée pour la sécurité des systèmes d'information

L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) est la personne juridiquement responsable, pour la DINUM, de la sécurité des systèmes d'information. L'AQSSI est unique pour tout le périmètre de la DINUM et sa responsabilité ne peut pas être déléguée.

L'AQSSI possède le pouvoir hiérarchique et la capacité d'arbitrage sur les moyens budgétaires et humains, employés pour que la sécurité numérique de l'entité se rapproche d'un état jugé optimal.

L'AQSSI de la DINUM est la directrice interministérielle du numérique[4]. Elle désigne le conseiller à la sécurité numérique avec qui elle échange régulièrement.

Article 7. L'autorité d'homologation

Désignée de manière formelle par l'AQSSI, l'autorité d'homologation est la personne qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire, prend la décision d'accepter les risques résiduels identifiés.

L'autorité d'homologation (AH) est membre du comité de direction de la DINUM afin de lui donner un niveau hiérarchique suffisant pour assumer les responsabilités liées à l'acceptation des risques résiduels identifiés sur le système d'information cible.

Article 8. Le fonctionnaire de sécurité des systèmes d'information

Placé auprès du haut fonctionnaire de défense adjoint et désigné par la Première ministre, le fonctionnaire de sécurité des systèmes d'information (FSSI) anime la chaîne fonctionnelle de sécurité numérique des SPM pour l'ensemble des activités qui lui sont dévolues.

Les missions du FSSI des SPM sont détaillées dans la PSSI des SPM mentionnée dans l'article 2.

Article 9. Le délégué à la protection des données

Placé auprès du secrétaire général du gouvernement, le délégué à la protection des données (DPD) des SPM est chargé de piloter la conformité aux lois et règlements relatifs à la protection des données personnelles pour l'ensemble des traitements mis en œuvre sur son périmètre de responsabilité.

Article 10. Le conseiller à la sécurité numérique

Placé auprès de l'AQSSI, le conseiller à la sécurité numérique (CSN) conseille et accompagne l'autorité qualifiée dans l'exercice de ses responsabilités.

Il assure des fonctions de conseil, de contrôle, de pilotage des risques et des processus d'homologation. A ce titre, il est l'interlocuteur privilégié de l'AQSSI et des AH concernant l'homologation des produits de la DINUM.

Il s'appuie sur les compétences internes à disposition en matière de sécurité numérique, notamment les différents correspondants à la sécurité des systèmes d'information (CSSI).

Il élabore et maintient à jour la présente politique et son corpus. Il élabore le rapport annuel de la sécurité numérique[5] pour le compte de l'AQSSI. Il dispose d'une délégation de pouvoir de la part de l'autorité qualifiée pour déposer, en son nom, toute plainte relative au domaine de la cybercriminalité[6].

---

[4] Conformément au paragraphe 3.2.3 de l'arrêté 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'Etat et de ses établissements publics.

[5] Voir Article 18

[6] La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication ou ciblant ces mêmes réseaux.

Il participe en tant que de besoin aux comités de direction afin de pouvoir éclairer les membres du comité sur les enjeux métiers en besoins de sécurité et les éventuels points d'attention, d'arbitrage ou de décision. A défaut, il remonte les éléments significatifs à chaque responsable de département ou, le cas échéant, directement à l'AQSSI.

Ils échangent régulièrement avec :

- Le FSSI des SPM, pour assurer un pilotage optimal des actions SSI de leurs périmètres ;
- Les FSSI ministériels, notamment concernant les alertes et incidents de sécurité pouvant impacter leur périmètre ;
- Le correspondant DINUM sur la protection des données et/ou avec le DPD des SPM, sur les aspects SSI relatifs à la protection des données à caractère personnel, en conformité avec le RGPD.

Il peut représenter l'autorité qualifiée dans les comités/instances ministériels ou interministériels de pilotage de la sécurité numérique.

Article 11. Le responsable de la sécurité des systèmes d'information

Le responsable de la sécurité des systèmes d'information (RSSI) est placé sous l'autorité de l'AQSSI. Il dispose d'une expertise technique en matière de sécurité numérique, lui permettant de conseiller et d'accompagner l'autorité qualifiée dans la mise en œuvre opérationnelle de la sécurité numérique.

Dans le contexte de la DINUM, le rôle de RSSI est directement assuré par le CSN. Il dispose de deux adjoints, répartis entre le périmètre spécifique du Réseau Interministériel de l'État (RIE) et le reste du périmètre de la DINUM, pour l'aider dans la réalisation de ses missions.

Le RSSI et ses adjoints conseillent et accompagnent les équipes produits dans leurs démarches d'homologation.

Article 12. Les correspondants à la sécurité des systèmes d'information

Les correspondants à la sécurité des systèmes d'information (CSSI) sont considérés comme des référents SSI au sein des équipes produits. Ils assistent le CSN dans l'accomplissement de ses missions.

Il est soit désigné par le responsable produit auprès duquel il exerce, soit auprès d'un chef de pôle pour un portefeuille défini de produits.

Il possède les connaissances métiers nécessaires à l'accomplissement des missions qui lui sont attribuées.

Article 13. Le centre opérationnel de sécurité des produits interministériels

En matière de défense des systèmes d'information de la DINUM, le centre opérationnel de sécurité des produits interministériels (CSIRT-DINUM) a comme missions principales :

- La supervision de la sécurité des produits interministériels de la DINUM ;
- La détection des cyberattaques sur les produits éligibles de la DINUM ;
- La coordination de la réponse aux incidents de sécurité ;
- La veille technologique sur les vulnérabilités des composants des différents produits ;
- L'alerte et l'information des différents acteurs SSI pour ce qui concerne les événements et incidents de sécurité relevant de leurs périmètres ;
- La coopération avec les autres CSIRT afin d'alimenter et améliorer la connaissance de l'état de la menace et partager les retours d'expérience pour faire face aux attaques à venir.

Les échanges avec les partenaires (gestion de crise, réponse aux incidents…) font systématiquement l'objet de protocoles formalisés.

Le CSIRT-DINUM assure la liaison opérationnelle avec les équipes de l'ANSSI et celles des différents systèmes d'information de la DINUM dont il assure la supervision de la sécurité.

TITRE II : Gouvernance interne de la sécurité numérique

Article 14. Gouvernance interne de la sécurité numérique

Le système de gouvernance de la sécurité numérique permet d'animer les processus stratégiques, de pilotage, d'arbitrage/décision et d'amélioration continue de la sécurité numérique. Il définit les règles et les priorités. Il permet la mise en œuvre cohérente et coordonnée de mesures spécifiques, fondées sur des capacités techniques et opérationnelles de prévention, de protection, de détection, en vue d'assurer la protection et la résilience des systèmes d'information, particulièrement en cas de cyberattaques.

Article 15. Comitologie

Au sein de la DINUM, trois niveaux de gouvernance de la sécurité numérique sont définis :

- Le comité de direction de la sécurité numérique, couvrant l'ensemble du périmètre de la DINUM ;
- Les comités de suivi de la sécurité numérique, permettant un état des lieux d'un système d'information spécifique de la DINUM ;
- Les groupes de travail de la sécurité numérique, qui permettent de travailler sur des thématiques particulières d'un système d'information de la DINUM.

Article 16. Comité de direction de la sécurité numérique

Un comité de direction de la sécurité numérique (CODIR SN) est organisé mensuellement et est présidée par l'autorité qualifiée. Les principaux rôles de ce comité sont de :

- Définir et arbitrer les orientations stratégiques relatives à la sécurité numérique et les moyens techniques et budgétaires associés ;
- Suivre l'état d'avancement des homologations des SI de la DINUM ;
- Faire le bilan des incidents significatifs et l'état des lieux des cybermenaces susceptibles d'affecter les systèmes de la DINUM ;
- Identifier les SI nécessitant une priorisation des actions de sécurité numérique.

Les membres de droit de ce comité sont :

- L'AQSSI et son adjoint ;
- Le CSN de la DINUM ;
- Le responsable du département « Infrastructures et services opérés » ;
- Le responsable du département « Opérateur des produits interministériels ».

Peuvent être invités sur demande de l'AQSSI :

- Le HFDS ou son adjoint ;
- Le FSSI des SPM ;
- Les autres responsables de département de la DINUM.

D'autres CODIR SN peuvent être organisés en tant que de besoin pour des produits spécifiques si cela est nécessaire aux processus de certification ou de qualification du produit concerné.

Article 17. Le comité de suivi de la sécurité numérique

Un comité de suivi de la sécurité numérique (COSEC) est organisé à une fréquence au moins semestrielle pour les systèmes d'information les plus sensibles de la DINUM. Ces comités sont présidés par un représentant de la maîtrise d'ouvrage du système d'information concerné.

Les principaux rôles de ce comité sont de :

- Suivre l'état d'avancement des mesures du plan d'action SSI, issues de l'analyse de risque et des audits ;
- Suivre les vulnérabilités et discuter des incidents de sécurité rencontrés ;
- Discuter des difficultés rencontrées et des évolutions à venir ;
- Identifier les sujets transverses de sécurité à discuter en CODIR SN.

Les membres de droit de ce comité sont :

- Les responsables de département et chefs de pôle concernés ;
- Le CSN de la DINUM ;
- Le responsable métier du système d'information.

En fonction des sujets abordés, peuvent être invités à ces comités :

- Le FSSI des SPM ;
- Les FSSI ministériels ;
- Les CSN / RSSI des principaux partenaires ;
- Des experts techniques du produit.

Article 18. Les groupes de travail de la sécurité numérique

Les groupes de travail de la sécurité numérique (GT SN) peuvent être organisés en fonction des besoins d'expertise sur un système d'information. Ils ont pour objectif de regrouper des experts techniques ou fonctionnels de la sécurité numérique, afin d'aider à la conception du système ou dans la résolution de problèmes. Ils traitent principalement des sujets liés aux appréciations des risques, aux audits de sécurité et au suivi des plans d'action.

Les GT SN sont organisés et planifiés en fonction des besoins de la maîtrise d'ouvrage du produit, qui est libre dans le choix des invités en fonction des expertises nécessaires.

Article 19. Rapport annuel de la sécurité numérique

Le rapport annuel de la sécurité numérique de la DINUM, transmis au HFDS des SPM, comprend les éléments suivants :

- Un état des lieux de la sécurité numérique des principaux SI de la DINUM ;
- Une synthèse des incidents de sécurité rencontrés ;
- Les ressources et moyens affectés à la sécurité numérique, ainsi que les formations et les actions de sensibilisation réalisées.

En fonction des demandes adressées par la chaîne SSI des SPM, de nouveaux éléments sont susceptibles de venir enrichir le rapport.

TITRE III : Maîtrise du risque numérique

Article 20. Principes stratégiques de la maîtrise du risque numérique

L'évolution du risque numérique dans l'action de l'État engage la responsabilité des autorités. Cette responsabilité est accentuée par l'émergence ou l'évolution de la réglementation (Règlement général sur la protection des données, dispositif sur la sécurité des secteurs d'activités d'importance vitale, protection du secret de la défense nationale, etc.).

Devant l'accroissement de la menace numérique et sa propension à gagner toutes les activités de la DINUM, les autorités doivent définir, sur leur périmètre de responsabilité de nouveaux seuils d'acceptabilité du risque. Ces risques ne sont pas limités au strict périmètre de la DINUM, mais concernent également son écosystème formé des prestataires, fournisseurs, sous-traitants, ministères partenaires, etc.

Cet écosystème numérique participe directement ou indirectement aux missions de la DINUM. Toute vulnérabilité sur cet écosystème doit être prise en compte dans la maîtrise du risque numérique.

Dans un esprit de conformité avec la doctrine[7] « Cloud au centre » de l'Etat, les informations sensibles doivent être hébergées dans des lieux d'hébergement maîtrisés, dont les procédures de sécurité sont connues et homologuées.

Article 21. Cartographie des SI

Les systèmes d'information sont de plus en plus complexes et interconnectés.

La cartographie vise à réaliser l'inventaire des actifs numériques des systèmes d'information de la DINUM, particulièrement pour les plus sensibles, et comprendre leurs liens et leur fonctionnement. C'est donc un outil stratégique, nécessaire à la maîtrise des systèmes d'information de la DINUM et de leurs écosystèmes.

Une cartographie maintenue à jour permet ainsi de :

- Disposer d'un inventaire à jour de l'ensemble des systèmes d'information (listes des briques logicielles et matérielles, architectures réseaux…) ;
- En complément de l'homologation, identifier les systèmes les plus essentiels et les plus exposés, facilitant la prise de décision lors des incidents ou des crises ;
- Anticiper les chemins d'attaque et de mettre en place les mesures adéquates ;
- Réagir plus efficacement en cas d'incident ou d'attaque, en permettant de qualifier les impacts et de prévoir les conséquences des actions défensives ;
- Assurer le maintien en condition opérationnelle et de sécurité des systèmes d'information.

[7] https://www.legifrance.gouv.fr/download/pdf/circ?id=45446

La cartographie d'un SI est à élaborer par chaque équipe produit et doit pouvoir être communiquée sur demande en cas d'audit ou de contrôle. Elle doit être tenue à disposition de l'ANSSI et du FSSI des SPM.

Article 22. Cartographie des risques numériques

La cartographie des risques de la DINUM est pilotée par le CSN. Elle est alimentée par les éléments remontés par les responsables de produits et les audits réalisés.

Le CSN maintient à jour cette cartographie pour son périmètre et remonte à l'AQSSI les risques jugés majeurs, persistants ou non. Sur demande du FSSI SPM, le CSN rend compte des risques impactant les SI de son périmètre.

Article 23. Intégration de la sécurité dans le cycle de vie des systèmes d'information

Dès le début des études préliminaires et jusqu'à leur décommissionnement, l'intégration de la sécurité dans les produits est placée sous l'entière responsabilité de l'AQSSI, qui s'appuie sur les responsables des produits pour appliquer la démarche définie par le CSN.

Cette intégration de la sécurité dès la conception et tout au long du cycle de vie d'un produit doit impliquer plusieurs points de vue, dont en particulier :

- La maîtrise d'ouvrage du produit qui doit exprimer ses besoins et les enjeux de sécurité ;
- Le responsable produit qui peut demander au CSN, des avis et conseils pour assurer un traitement des risques adapté aux enjeux et cohérent avec la PSN-DINUM ;
- Le CSN, qui contrôle pour la DINUM que tous les produits ont intégré les considérations de sécurité pour eux-mêmes et pour leur écosystème. Il doit alerter l'AQSSI s'il considère que les risques résiduels ne sont pas suffisamment traités par le produit et qu'ils peuvent avoir un impact significatif sur la DINUM ou son écosystème.

Article 24. Maîtrise des prestataires, fournisseurs et partenaires

L'AQSSI s'assure du traitement des risques que les activités des tiers (prestataires, fournisseurs ou partenaires) font peser sur ses systèmes d'information.

Pour cela, les clauses de sécurité sont insérées dans les contrats ou conventions de services permettant l'engagement des tiers à répondre aux objectifs de sécurité des produits. Pour maintenir un niveau de confiance suffisant des dispositions prises par les tiers, il est essentiel de procéder à des revues régulières de l'application de ces clauses.

Des clauses contractuelles types de sécurité sont proposées dans le corpus de la sécurité numérique.

Article 25. Homologation de sécurité

Le décret n°2022-513[8] du 8 avril 2022 dispose que l'homologation de sécurité s'applique aux infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat.

L'homologation de sécurité est une décision formelle prise par l'AQSSI ou par toute personne qu'elle aura désigné comme autorité d'homologation.

L'homologation permet d'attester que :

- Les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour maîtriser ces risques sont mises en œuvre ;
- Les éventuels risques résiduels ont été acceptés par l'autorité d'homologation.

Toute homologation d'un système d'information doit être formalisée dans une note rappelant le périmètre de l'homologation, la durée, les éventuelles réserves voire dérogations à la présente politique. Ce document doit être systématiquement communiqué au FSSI des SPM.

Tout au long du cycle de vie du SI, le processus d'homologation permet de maintenir le risque de sécurité numérique à un niveau adapté et acceptable.

Les risques pesant sur un SI doivent être périodiquement réévalués dans une démarche permanente d'amélioration continue et d'adaptation à l'évolution de la menace. A ce titre, une homologation a nécessairement une durée limitée dans le temps.

Dans le cas d'une responsabilité partagée entre plusieurs AQSSI, c'est celle désignée comme compétente sur le domaine de la sécurité numérique qui désigne l'AH. A défaut, les AQSSI s'accordent pour désigner une AH commune. Les AH sont directement subordonnées aux AQSSI compétentes et sont responsables de la conduite des missions pour lesquelles le système est créé. La DINUM reste en charge du secrétariat des commissions d'homologation des systèmes d'information concernés.

La démarche d'homologation type de la DINUM est détaillée au sein du corpus de la sécurité numérique.

La prise en compte des obligations du présent article pour les infrastructures et services logiciels informatiques de la DINUM fait l'objet d'une note interne.

Article 26. Systèmes d'information critiques

Au sein de la DINUM, certains systèmes d'information sont réglementés par des arrêtés et/ou des directives européennes :

- Arrêté[9] du 29 mai 2019 fixant les règles de sécurité et les modalités de déclaration des SIIV et des incidents de sécurité relatives au secteur d'activités d'importance « Activités civiles de l'État » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense ;

[8] Décret relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693
[9] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038565011/

- Directive NIS 2[10].

Tout responsable d'un produit de la DINUM est garant de l'application de la réglementation sur le système d'information dont il a la charge.

[10] https://cyber.gouv.fr/la-directive-nis-2

TITRE IV : Gestion de crise et continuité d'activité

Article 27. Gestion de crise

La maîtrise de la gestion de crise est primordiale au sein de la DINUM. L'émergence du numérique dans ses missions implique que l'organisation et les procédures internes de gestion de crise doivent être adaptées pour y incorporer la dimension numérique comme un facteur naturellement transverse.

L'AQSSI doit se préparer à la gestion d'incidents de sécurité numérique susceptibles de déclencher une crise. En particulier, des réponses aux scénarios de cyberattaques critiques doivent être préparées en s'appuyant sur un plan de gestion de crise

Le plan gestion de crise et ses déclinaisons opérationnelles, font partie des livrables du corpus de la présente PSN-DINUM.

Article 28. Plan de continuité d'activité

Le plan de continuité d'activité (PCA) constitue un chapitre essentiel de la politique de sécurité d'une entité. Il doit pleinement intégrer le risque numérique. Il doit être revu, testé, et enrichi à intervalles réguliers pour rester activable efficacement à tout moment.

L'AQSSI définit la stratégie de PCA et engage les moyens nécessaires (humains, techniques et logistiques) pour sa mise en œuvre. Elle nomme un responsable du PCA (RPCA) qui assure, en lien avec le CSN, la bonne mise en œuvre des dispositions prévues dans celui-ci et veille également à son maintien en condition opérationnelle.

Tout produit, dès lors qu'il dispose d'enjeux forts de disponibilité et/ou d'intégrité, doit être inscrit au PCA de la DINUM et élaborer les procédures opérationnelles utiles à sa propre résilience (plan de reprise d'activité, plan de secours informatique…). Les dispositions garantissant la continuité de service (passage en mode dégradé, mesures de contournement, retour à la normale…) doivent être établies avec les maîtrises d'ouvrage concernées.

TITRE V : Dispositions opérationnelles

Les dispositions opérationnelles reposent sur les 4 objectifs suivants : prévenir, protéger, détecter et répondre aux cyberattaques.

Article 29. Prévention des scénarios de risque

La plupart des attaques informatiques utilisent successivement plusieurs techniques de propagation.

La prévention permet de limiter la survenue des incidents de sécurité en réduisant la probabilité qu'un scénario de risque se réalise entièrement.

Le dispositif de prévention mis en œuvre au sein de la DINUM repose principalement sur :

- La sensibilisation et la formation des personnels, tant internes qu'externes ;
- L'homologation des systèmes d'information avant leur mise en production ou avant toute mise en production d'une évolution significative ;
- Le maintien en condition opérationnelle et de sécurité des produits qui doit permettre a minima d'assurer :
    - Une veille technologique pour recenser les vulnérabilités effectives ou potentielles sur les actifs logiciels des produits ;
    - La mise en place d'actions préventives ou correctives pour traiter la vulnérabilité ou en diminuer les impacts.
- Le maintien de l'homologation durant tout le cycle de vie des produits.

Article 30. Protection des systèmes d'information

La protection vise à limiter l'impact direct des attaques de sécurité et freiner leur propagation au sein du système d'information.

Le corpus de la PSN liste les règles élémentaires de sécurité qui doivent être appliquées pour répondre à cet objectif. La démarche d'homologation permet d'identifier les mesures à mettre en place pour protéger les actifs essentiels des systèmes d'information de la DINUM.

Des dispositions opérationnelles relatives à la protection des systèmes d'information sont également décrites au sein du corpus de la sécurité numérique.

Article 31. Détection et analyse des évènements de sécurité

La détection et l'analyse des évènements de sécurité, permettant la qualification d'un incident de sécurité, doivent permettre d'en limiter les impacts au travers d'une réponse adaptée. Ce dispositif permet d'étudier les modes opératoires des attaquants en vue de s'en prémunir.

Au sein de la DINUM, dès lors qu'un SI présente de forts enjeux, il doit être intégré dans un dispositif permettant d'assurer la supervision de sa sécurité et la détection des évènements redoutés.

Des dispositions opérationnelles relatives à la détection sont décrites au sein du corpus de la sécurité numérique.

Article 32. Réponse aux attaques

La réponse aux attaques est coordonnée par le CSN de la DINUM, en lien avec les responsables produits, le FSSI des SPM, l'ANSSI et notamment le CERT-FR.

Une réponse adaptée aux attaques comprend non seulement la gestion technique assurée par les équipes opérationnelles, éventuellement appuyées par le CSIRT-DINUM, mais également la continuité des activités des équipes produits, la relation avec les autorités et la communication avec les parties prenantes et les instances judiciaires.

Les dispositifs dont se dote la DINUM pour répondre à ces enjeux reposent sur des procédures de gestion d'incident et de crise, permettant :

- La priorisation des besoins de cloisonnement et de reprise sur le périmètre DINUM ;
- La mise en œuvre d'une stratégie de communication adaptée et partagée ;
- La réalisation d'exercices réguliers de crise, impliquant les personnels et les systèmes d'information dont ils sont responsables.

La traçabilité des actions engagées à l'occasion d'une réponse aux attaques est essentielle à la capitalisation des connaissances et à l'analyse à froid de l'évolution des menaces. Son objectif est de garantir, de manière durable, la qualité et la sécurité du service offert aux utilisateurs finaux, agents publics ou citoyens.

Des dispositions opérationnelles relatives à la réponse aux attaques sont décrites au sein du corpus de la sécurité numérique.

FIN DU DOCUMENT