BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 57 du 22 décembre 2016

TEXTE SIGNALE

ARRÊTÉ

fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Finances » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

Du *28 novembre 2016*

PREMIER MINISTRE.

ARRÊTÉ fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Finances » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

Du 28 novembre 2016

NOR P R M D 1 6 3 0 7 2 2 A

Pièce(s) Jointe(s) :

Une annexe.

Classement dans l'édition méthodique : BOEM 160.4.3

Référence de publication : JO n° 281 du 3 décembre 2016, texte n° 3 ; signalé au BOC 57/2016.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « *Finances* » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

NOR : *PRMD1630722A*

Publics concernés : *opérateurs d'importance vitale mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense relevant du secteur d'activités d'importance vitale « Finances » ; prestataires de service de confiance mentionnés dans le décret n° 2015-350 du 27 mars 2015.*

Objet : *règles de sécurité prévues à l'article L. 1332-6-1 du code de la défense ; modalités de déclaration des systèmes d'information d'importance vitale mentionnés à l'article R. 1332-41-2 du même code ; modalités de déclaration des incidents de sécurité mentionnés à l'article R. 1332-41-10 du même code.*

Entrée en vigueur : *le texte entre en vigueur le 1er janvier 2017.*

Notice : *l'arrêté fixe les règles de sécurité que les opérateurs d'importance vitale sont tenus de respecter pour protéger leurs systèmes d'information (annexe I), les délais dans lesquels les opérateurs sont tenus d'appliquer les règles de sécurité (annexe II), les modalités selon lesquelles les opérateurs déclarent à l'Agence nationale de la sécurité des systèmes d'information la liste de leurs systèmes d'information d'importance vitale identifiés par types de système (annexe III), ainsi que les modalités selon lesquelles les opérateurs déclarent à l'agence certains types d'incidents affectant la sécurité ou le fonctionnement de leurs systèmes d'information (annexe IV).*

Références : *l'arrêté est pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense. Il peut être consulté sur le site Légifrance (http: //www.legifrance.gouv.fr) à l'exception de ses annexes II, III et IV qui ne sont pas publiées. Ces annexes sont notifiées aux personnes ayant besoin d'en connaître.*

Le Premier ministre,

Vu le code de la défense, notamment ses articles L. 1332-1 et suivants, L. 2321-1, R.* 1132-3, R. 1332-3, R. 1332-4, R. 1332-41-1 et suivants et R. 2311-1 et suivants ;

Vu le code pénal, notamment ses articles 226-13 et 413-9 ;

Vu 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 » ;

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ;

Vu l'arrêté du 2 juin 2006 modifié fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs ;

Vu l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale ;

Vu l'avis du comité consultatif de la législation et de la réglementation financières en date du 13 octobre 2016 ;

Vu l'avis du ministre chargé de l'économie et des finances en date du 30 septembre 2016,

Arrête :

CHAPITRE Ier

Règles de sécurité

Art. 1er. – Les règles de sécurité prévues à l'article L. 1332-6-1 du code de la défense relatives au secteur d'activités d'importance vitale « *Finances* » figurent à l'annexe I du présent arrêté.

A compter de l'entrée en vigueur du présent arrêté ou de sa date de désignation en tant qu'opérateur d'importance vitale conformément aux dispositions de l'article R. 1332-3 du code de la défense, tout opérateur d'importance vitale relevant du secteur mentionné au premier alinéa applique ces règles de sécurité dans les délais qui figurent à l'annexe II.

Chapitre II

Déclaration des systèmes d'information d'importance vitale

Art. 2. – Dans un délai de trois mois à compter de la date d'entrée en vigueur du présent arrêté ou de sa désignation comme opérateur d'importance vitale conformément aux dispositions de l'article R. 1332-3 du code de la défense, tout opérateur relevant du secteur d'activités d'importance vitale « *Finances* » adresse par courrier à l'Agence nationale de la sécurité des systèmes d'information la liste de systèmes d'information d'importance vitale prévue à l'article R. 1332-41-2 du code de la défense, ainsi que, pour chaque système, le formulaire de déclaration disponible sur le site internet de l'agence (www.ssi.gouv.fr).

Pour déterminer si un système d'information peut être qualifié d'importance vitale au sens des dispositions de l'article L. 1332-6-1 du code de la défense, l'opérateur d'importance vitale mène une analyse d'impacts sur ses systèmes d'information, notamment ceux relevant des types de système d'information mentionnés à l'annexe III du présent arrêté.

Lorsque, pour un type de système d'information mentionné à l'annexe III du présent arrêté, l'opérateur ne déclare aucun système d'information d'importance vitale relevant de ce type de système, il en précise les raisons.

Art. 3. – L'opérateur d'importance vitale communique une fois par an à l'Agence nationale de la sécurité des systèmes d'information les mises à jour de sa liste et des formulaires de déclaration.

Il déclare tout nouveau système d'information d'importance vitale préalablement à sa mise en service et tout système d'information qui satisfait aux conditions pour être qualifié d'importance vitale postérieurement à sa mise en service dès qu'il satisfait à ces conditions.

Il informe sans délai l'Agence nationale de la sécurité des systèmes d'information de tout retrait de sa liste d'un des systèmes précédemment déclarés et en précise les raisons.

Chapitre III

Déclaration des incidents de sécurité

Art. 4. – En application de l'article R. 1332-41-10 du code de la défense, tout opérateur relevant du secteur d'activités d'importance vitale « *Finances* » déclare chaque incident qui relève d'un type figurant à l'annexe IV du présent arrêté. Il adresse à cet effet à l'Agence nationale de la sécurité des systèmes d'information le formulaire de déclaration disponible sur le site internet de l'agence (www.ssi.gouv.fr) selon le moyen approprié à la sensibilité des informations déclarées.

Le formulaire est un document confidentiel susceptible de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Il est, le cas échéant, couvert par le secret de la défense nationale.

Chapitre IV

Dispositions finales

Art. 5. – Tout opérateur d'importance vitale relevant du secteur d'activités d'importance vitale « *Finances* » communique à l'Agence nationale de la sécurité des systèmes d'information les coordonnées de la personne mentionnée à l'article R. 1332-41-20 du code de la défense dans un délai de trois mois à compter de l'entrée en vigueur du présent arrêté ou de sa désignation comme opérateur d'importance vitale conformément aux dispositions de l'article R. 1332-3 du code de la défense.

Art. 6. – Les dispositions du présent arrêté entrent en vigueur le 1er janvier 2017.

Art. 7. – Le présent arrêté n'est pas applicable aux services de l'Etat désignés en tant qu'opérateurs d'importance vitale du secteur d'activités d'importance vitale « *Finances* ».

Art. 8. – Le directeur général de l'Agence nationale de la sécurité des systèmes d'information est chargé de l'exécution du présent arrêté qui sera publié au *Journal officiel* de la République française à l'exception de ses annexes II, III et IV. Ces annexes sont notifiées aux personnes ayant besoin d'en connaître par le directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Fait le 28 novembre 2016.

Pour le Premier ministre et par délégation :
Le secrétaire général de la défense et de la sécurité nationale,
L. Gautier

ANNEXE I

RÈGLES DE SÉCURITÉ RELATIVES AU SECTEUR D'ACTIVITÉS D'IMPORTANCE VITALE « FINANCES »

1. **Règle relative à la politique de sécurité des systèmes d'information**

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une politique de sécurité des systèmes d'information (PSSI).

La PSSI décrit l'ensemble des moyens organisationnels et techniques mis en œuvre par l'opérateur afin d'assurer la sécurité de ses systèmes d'information d'importance vitale (SIIV). En particulier, elle :

- précise les objectifs et les orientations stratégiques en matière de sécurité des SIIV ;
- décrit l'organisation de la gouvernance de la sécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe (prestataires, fournisseurs, etc.) à l'égard de la sécurité des SIIV ;
- prévoit un plan de sensibilisation à la sécurité des SIIV au profit de l'ensemble du personnel ainsi qu'un plan de formation à la sécurité des SIIV au profit des personnes ayant des responsabilités particulières, notamment les personnes en charge de l'administration et de la sécurité des SIIV et les utilisateurs disposant de droits d'accès privilégiés aux SIIV ;
- fixe les mesures de sécurité générales, notamment en matière de contrôle du personnel interne et du personnel externe, de sécurité physique des SIIV, de gestion des ressources matérielles et logicielles, de gestion de l'assistance technique, de contrôle d'accès aux SIIV, d'exploitation et d'administration des SIIV, de cryptographie, de sécurité des communications et de sécurité des processus de développement ;
- définit les procédures suivantes :
  - la procédure d'homologation de sécurité des SIIV ;
  - les procédures d'évaluation des risques en matière de sécurité des SIIV ;
  - les procédures de contrôle et d'audit de la sécurité des SIIV ;
  - la procédure de maintien en conditions de sécurité des ressources des SIIV ;
  - la procédure de traitement des incidents de sécurité ;
  - les procédures de gestion de crises en cas d'attaques informatiques et de continuité d'activité.

La PSSI et ses documents d'application sont approuvés formellement par la direction de l'opérateur. L'opérateur élabore au profit de sa direction, au moins annuellement, un rapport sur la mise en œuvre de la PSSI et de ses documents d'application. Ce rapport précise notamment l'état des lieux des risques, le niveau de sécurité des SIIV et les actions de sécurisation menées.

La PSSI, ses documents d'application et les rapports sur leur mise en œuvre sont tenus à la disposition de l'Agence nationale de la sécurité des systèmes d'information.

2. **Règle relative à l'homologation de sécurité**

L'opérateur d'importance vitale procède à l'homologation de sécurité de chaque système d'information d'importance vitale (SIIV), en mettant en œuvre la procédure d'homologation prévue par sa politique de sécurité des systèmes d'information (PSSI).

L'homologation d'un système est une décision formelle prise par l'opérateur qui atteste que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'opérateur.

Dans le cadre de l'homologation, un audit de la sécurité du SIIV doit être réalisé. Cet audit vise à vérifier l'application et l'efficacité des mesures de sécurité du SIIV et notamment le respect des règles de sécurité mentionnées dans le présent arrêté. L'audit doit permettre d'évaluer le niveau de sécurité du SIIV au regard des menaces et des vulnérabilités connues. Il comporte notamment la réalisation d'un audit d'architecture, d'un audit de configuration, d'un audit organisationnel et physique et de tests de vulnérabilité et d'intrusion.

Cet audit est réalisé dans le respect des règles fixées par le référentiel en matière d'audit de sécurité des systèmes d'information prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

L'opérateur peut réaliser lui-même l'audit ou recourir à un prestataire qualifié dans les conditions prévues au chapitre III du décret n° 2015-350 du 27 mars 2015 précité.

A l'issue de l'audit, l'opérateur ou, le cas échéant, le prestataire élabore un rapport d'audit qui expose les constatations sur les mesures appliquées et sur le respect des règles de sécurité prévues par le présent arrêté. Le rapport précise si le niveau de sécurité atteint est conforme aux objectifs de sécurité, compte tenu des menaces et des vulnérabilités connues. Il formule des recommandations pour remédier aux éventuelles non-conformités et vulnérabilités découvertes.

L'opérateur prend la décision d'homologuer un SIIV sur la base du dossier d'homologation comportant notamment :

- l'analyse de risques et les objectifs de sécurité du SIIV ;
- les mesures de sécurité appliquées au SIIV ;
- les rapports d'audit de la sécurité du SIIV ;
- les risques résiduels et les raisons justifiant leur acceptation.

L'homologation est valable pour une durée maximale de trois ans et est renouvelée au terme de cette période. Toutefois, la validité de l'homologation est réexaminée par l'opérateur lors de chaque événement ou évolution de nature à modifier le contexte décrit dans le dossier d'homologation.

L'opérateur tient à la disposition de l'Agence nationale de la sécurité des systèmes d'information les décisions et dossiers d'homologation, notamment les rapports d'audit. Ces documents confidentiels sont susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.

La présente règle relative à l'homologation s'applique sans préjudice des dispositions prévues par l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, en matière d'homologation des systèmes d'information traitant des informations classifiées.

3. **Règle relative à la cartographie**

L'opérateur d'importance vitale doit être en mesure de fournir à l'Agence nationale de la sécurité des systèmes d'information, pour chaque système d'information d'importance vitale (SIIV), les éléments de cartographie suivants :

- l'architecture applicative, comprenant notamment les noms et les fonctions des applications, des bases de données et des services installés sur le SIIV ;
- l'architecture système, comprenant notamment l'inventaire et l'architecture des dispositifs d'administration du SIIV permettant de réaliser les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- l'architecture réseau, comprenant notamment :
  - les plages d'adresses IP de sortie du SIIV vers internet ou un réseau tiers, ou accessibles depuis ces réseaux ;
  - la cartographie des flux d'accès au SIIV (adresses IP sources et destinations, ports de destination) ;
- la liste des comptes disposant de droits d'accès privilégiés (appelés « comptes privilégiés ») au SIIV. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés, notamment les comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de messagerie, comptes de processus, etc.).

Les éléments de cartographie ainsi réunis sont des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.

Sur demande de l'Agence nationale de la sécurité des systèmes d'information, l'opérateur lui communique les éléments de cartographie mis à jour sur un support électronique, dans un format qui peut être lu par les principaux logiciels bureautiques accessibles au public.

4. **Règle relative au maintien en conditions de sécurité**

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de maintien en conditions de sécurité des ressources matérielles et logicielles de ses systèmes d'information d'importance vitale (SIIV), conformément à sa politique de sécurité des systèmes d'information.

Cette procédure définit les conditions permettant de maintenir le niveau de sécurité des ressources des SIIV en fonction de l'évolution des vulnérabilités et des menaces et notamment la politique d'installation de toute nouvelle version et mesure correctrice de sécurité d'une ressource et les vérifications à effectuer avant l'installation. Elle prévoit que :

- l'opérateur se tient informé des vulnérabilités et des mesures correctrices de sécurité susceptibles de concerner les ressources matérielles et logicielles de ses SIIV ;
- sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur installe et maintient toutes les ressources matérielles et logicielles de ses SIIV dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité ;
- préalablement à l'installation de toute nouvelle version, l'opérateur s'assure de l'origine de cette version et de son intégrité, et analyse l'impact de cette version sur le SIIV concerné d'un point de vue technique et opérationnel ;
- dès qu'il a connaissance d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur en planifie l'installation après avoir effectué les vérifications mentionnées à l'alinéa précédent, et procède à cette installation dans les délais prévus par cette procédure ;
- lorsque des raisons techniques ou opérationnelles le justifient, l'opérateur peut décider, pour certaines ressources de ses SIIV, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'opérateur met en œuvre des mesures techniques ou organisationnelles prévues par cette procédure pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues. L'opérateur décrit dans le dossier d'homologation du SIIV concerné ces mesures de réduction des risques et les raisons techniques ou opérationnelles ayant empêché l'installation d'une version supportée ou d'une mesure correctrice de sécurité.

5. **Règle relative à la journalisation**

L'opérateur d'importance vitale met en œuvre sur chaque système d'information d'importance vitale (SIIV) un système de journalisation qui enregistre les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SIIV ainsi qu'au fonctionnement du SIIV.

Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés au 1er alinéa :

- les serveurs applicatifs supportant les activités d'importance vitale ;
- les serveurs d'infrastructure système ;

– les serveurs d'infrastructure réseau ;
– les équipements de sécurité ;
– les postes d'ingénierie et de maintenance des systèmes industriels ;
– les équipements réseau ;
– les postes d'administration.

Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées. Ils sont, pour chaque SIIV, centralisés et archivés pendant une durée d'au moins six mois. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

6. **Règle relative à la corrélation et l'analyse de journaux**

L'opérateur d'importance vitale met en œuvre un système de corrélation et d'analyse de journaux qui exploite les événements enregistrés par le système de journalisation installé sur chacun des systèmes d'information d'importance vitale (SIIV), afin de détecter des événements susceptibles d'affecter la sécurité des SIIV.

Le système de corrélation et d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection d'événements susceptibles d'affecter la sécurité des systèmes d'information.

L'opérateur ou le prestataire mandaté à cet effet installe et exploite ce système de corrélation et d'analyse de journaux en s'appuyant sur les exigences du référentiel en matière de détection des incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

7. **Règle relative à la détection**

L'opérateur d'importance vitale met en œuvre, en application de l'article R. 1332-41-3 du code de la défense, un système de détection qualifié de type « sonde d'analyse de fichiers et de protocoles ».

Les sondes d'analyse de fichiers et de protocoles analysent les flux de données transitant par ces sondes afin de rechercher des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale (SIIV). Elles sont positionnées de manière à pouvoir analyser l'ensemble des flux échangés entre les SIIV et les systèmes d'information tiers à ceux de l'opérateur.

Les systèmes de détection qualifiés de ce type sont choisis parmi ceux figurant sur la liste prévue à l'article R. 1332-41-9 du code de la défense.

Ces systèmes de détection sont exploités selon les règles fixées par le référentiel en matière de détection des incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Ils sont exploités par un service de l'Etat ou un prestataire qualifié à cet effet dans les conditions prévues par le décret précité.

La présente règle relative à la détection ne s'applique pas aux SIIV relevant des types de système suivants :

– systèmes d'information assurant la sécurité physique des points d'importance vitale prévus à l'article R. 1332-4 du code de la défense ;
– systèmes d'information de gestion technique de bâtiment indispensables au fonctionnement des installations des points d'importance vitale prévus à l'article R. 1332-4 du code de la défense.

8. **Règle relative au traitement des incidents de sécurité**

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de traitement des incidents affectant le fonctionnement ou la sécurité de ses systèmes d'information d'importance vitale (SIIV), conformément à sa politique de sécurité des systèmes d'information.

L'opérateur ou le prestataire mandaté à cet effet procède au traitement des incidents en s'appuyant sur les exigences du référentiel en matière de réponse aux incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

Un système d'information spécifique doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système est cloisonné vis-à-vis du SIIV concerné par l'incident.

L'opérateur conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'au moins six mois. Il tient ces relevés techniques à la disposition de l'Agence nationale de la sécurité des systèmes d'information.

Les relevés techniques sont des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.

9. **Règle relative au traitement des alertes**

L'opérateur d'importance vitale met en place un service de permanence lui permettant de prendre connaissance, à tout moment et sans délai, d'informations transmises par l'Agence nationale de la sécurité des systèmes d'information relatives à des incidents, des vulnérabilités et des menaces. Il met en œuvre une procédure pour traiter les informations ainsi reçues et le cas échéant prendre les mesures de sécurité nécessaires à la protection de ses systèmes d'information d'importance vitale (SIIV).

L'opérateur communique à l'Agence nationale de la sécurité des systèmes d'information les coordonnées (nom du service, numéro de téléphone et adresse électronique) tenues à jour du service de permanence prévu à l'alinéa précédent.

10. **Règle relative à la gestion de crises**

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de gestion de crises en cas d'attaques informatiques majeures, conformément à sa politique de sécurité des systèmes d'information.

Cette procédure décrit les moyens techniques et organisationnels dont dispose l'opérateur pour mettre en œuvre les mesures décidées par le Premier ministre en cas de crises, notamment les mesures suivantes :

- appliquer une configuration système afin d'éviter les attaques ou d'en limiter les effets. Cette configuration peut viser notamment :
  - à proscrire l'utilisation de supports de stockage amovibles ou la connexion d'équipements nomades aux systèmes d'information de l'opérateur ;
  - à installer une mesure correctrice de sécurité sur un système d'information particulier ;
  - à imposer un protocole de routage ;
  - mettre en place des règles de filtrage sur les réseaux ou des configurations particulières sur les équipements terminaux. Cette mesure peut viser notamment :
    - à effectuer des restrictions d'accès sous forme de listes blanches et de listes noires d'utilisateurs ;
    - à bloquer les échanges de fichiers d'un type particulier ;
    - à isoler de tout réseau des sites internet, des applications, ou des équipements informatiques de l'opérateur en sollicitant le cas échéant l'appui des opérateurs publics de communications électroniques ;
  - isoler du réseau internet les systèmes d'information de l'opérateur. Cette mesure impose de déconnecter physiquement ou logiquement les interfaces réseau des systèmes d'information concernés.

La procédure précise les conditions dans lesquelles ces mesures peuvent être appliquées compte tenu des contraintes notamment techniques et organisationnelles de mise en œuvre.

11. **Règle relative à l'identification**

L'opérateur d'importance vitale crée des comptes individuels pour les utilisateurs et pour les processus automatiques accédant aux ressources de ses systèmes d'information d'importance vitale (SIIV).

Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, l'opérateur met en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes. Dans ce cas, l'opérateur décrit ces mesures dans le dossier d'homologation du SIIV concerné et les raisons justifiant le recours à des comptes partagés.

L'opérateur désactive sans délai les comptes qui ne sont plus nécessaires.

12. **Règle relative à l'authentification**

L'opérateur d'importance vitale protège les accès aux ressources de ses systèmes d'information d'importance vitale (SIIV), que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification basé sur un élément secret.

L'opérateur définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion des éléments secrets d'authentification mis en œuvre dans ses SIIV.

Lorsque la ressource le permet techniquement, les éléments secrets d'authentification doivent pouvoir être modifiés par l'opérateur chaque fois que cela est nécessaire. Dans ce cas, l'opérateur respecte les règles suivantes :

- l'opérateur doit modifier les éléments secrets d'authentification lorsqu'ils ont été installés par le fabricant ou le fournisseur de la ressource, avant sa mise en service. A cet effet, l'opérateur s'assure auprès du fabricant ou du fournisseur qu'il dispose des moyens et des droits permettant de réaliser ces opérations ;
- l'élément secret d'authentification d'un compte partagé doit être renouvelé régulièrement et à chaque retrait d'un utilisateur de ce compte ;
- les utilisateurs qui n'en ont pas la responsabilité, ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair ;
- lorsque les éléments secrets d'authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre comptes privilégiés ou entre un compte privilégié et un compte non privilégié ;
- lorsque les éléments secrets d'authentification sont des mots de passe, ceux-ci sont conformes aux règles de l'art telles que celles préconisées par l'Agence nationale de la sécurité des systèmes d'information, en matière de complexité (longueur du mot de passe et types de caractères), en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de renouvellement.

Lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'opérateur met en place un contrôle d'accès physique à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe. L'opérateur décrit dans le dossier d'homologation du SIIV concerné ces mesures et les raisons techniques ayant empêché la modification de l'élément secret d'authentification.

13. **Règle relative aux droits d'accès**

L'opérateur d'importance vitale définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion et d'attribution des droits d'accès aux ressources de ses systèmes d'information d'importance vitale (SIIV), et respecte les règles suivantes :

– l'opérateur n'attribue à un utilisateur ou à un processus automatique les droits d'accès à une ressource que si cet accès est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique ;
– l'opérateur définit les accès aux différentes fonctionnalités de cette ressource et en attribue les droits uniquement aux utilisateurs et aux processus automatiques qui en ont strictement le besoin ;
– les droits d'accès sont révisés périodiquement, au moins tous les ans, par l'opérateur. Cette révision porte sur les liens entre les comptes, les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet ;
– l'opérateur établit et tient à jour la liste des comptes privilégiés. Toute modification d'un compte privilégié (ajout, suppression, suspension ou modification des droits associés) fait l'objet d'un contrôle formel de l'opérateur destiné à vérifier que les droits d'accès aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège (seuls les droits strictement nécessaires sont accordés) et en cohérence avec les besoins d'utilisation du compte.

14. **Règle relative aux comptes d'administration**

L'opérateur d'importance vitale crée des comptes (appelés « comptes d'administration ») destinés aux seules personnes (appelées administrateurs) chargées d'effectuer les opérations d'administration (installation, configuration, gestion, maintenance, supervision, etc.) des ressources de ses systèmes d'information d'importance vitale (SIIV).

L'opérateur définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion et d'attribution des comptes d'administration de ses SIIV, et respecte les règles suivantes :

– l'attribution des droits aux administrateurs respecte le principe du moindre privilège. En particulier, afin de limiter la portée de ces droits individuels, ils sont attribués à chaque administrateur en les restreignant autant que possible au périmètre fonctionnel et technique dont cet administrateur est responsable ;
– un compte d'administration est utilisé exclusivement pour se connecter à un système d'information d'administration (système d'information utilisé pour les opérations d'administration des ressources) ou à une ressource administrée ;
– les opérations d'administration sont effectuées exclusivement à partir de comptes d'administration, et inversement, les comptes d'administration sont utilisés exclusivement pour les opérations d'administration ;
– lorsque l'administration d'une ressource ne peut pas techniquement être effectuée à partir d'un compte spécifique d'administration, l'opérateur met en place des mesures permettant d'assurer la traçabilité et le contrôle des opérations d'administration réalisées sur cette ressource et des mesures de réduction du risque lié à l'utilisation d'un compte non spécifique à l'administration. Il décrit dans le dossier d'homologation du SIIV concerné ces mesures ainsi que les raisons techniques ayant empêché l'utilisation d'un compte d'administration ;
– l'opérateur établit et tient à jour la liste des comptes d'administration de ses SIIV et les gère en tant que comptes privilégiés.

15. **Règle relative aux systèmes d'information d'administration**

L'opérateur d'importance vitale applique les règles suivantes aux systèmes d'information utilisés pour effectuer l'administration de ses systèmes d'information d'importance vitale (SIIV), qui sont appelés « systèmes d'information d'administration » :

– les ressources matérielles et logicielles des systèmes d'information d'administration sont gérées et configurées par l'opérateur ou, le cas échéant, par le prestataire qu'il a mandaté pour réaliser les opérations d'administration ;
– les ressources matérielles et logicielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des opérations d'administration. Cependant, lorsque des raisons techniques ou organisationnelles le justifient, le poste de travail physique de l'administrateur peut être utilisé pour réaliser des opérations autres que des opérations d'administration. Dans ce cas, des mécanismes de durcissement du système d'exploitation du poste de travail et de cloisonnement doivent être mis en place pour permettre d'isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel utilisé pour les opérations d'administration ;
– un environnement logiciel utilisé pour effectuer des opérations d'administration ne doit pas être utilisé à d'autres fins, comme l'accès à des sites ou serveurs de messagerie sur internet ;
– un utilisateur ne doit pas se connecter à un système d'information d'administration au moyen d'un environnement logiciel utilisé pour d'autres fonctions que des opérations d'administration ;
– les flux de données associés à des opérations autres que des opérations d'administration doivent, lorsqu'ils transitent sur les systèmes d'information d'administration, être cloisonnés au moyen de mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;
– les systèmes d'information d'administration sont connectés aux ressources à administrer au travers d'une liaison réseau physique utilisée exclusivement pour les opérations d'administration. Ces ressources sont

administrées au travers de leur interface d'administration physique. Lorsque des raisons techniques empêchent d'administrer une ressource au travers d'une liaison réseau physique ou de son interface d'administration physique, l'opérateur met en œuvre des mesures de réduction du risque telles que des mesures de sécurité logique. Dans ce cas, il décrit ces mesures et leurs justificatifs dans le dossier d'homologation du SIIV concerné ;

– lorsqu'ils ne circulent pas dans le système d'information d'administration, les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information. Si le chiffrement et l'authentification de ces flux ne sont pas possibles pour des raisons techniques, l'opérateur met en œuvre des mesures permettant de protéger ces flux en confidentialité et en intégrité et de renforcer le contrôle et la traçabilité des opérations d'administration. Dans ce cas, il décrit ces mesures et leurs justificatifs dans le dossier d'homologation du SIIV concerné ;

– les journaux enregistrant les événements générés par les ressources utilisées par les administrateurs ne contiennent aucun mot de passe en clair ou sous forme de condensat.

16. **Règle relative au cloisonnement**

L'opérateur d'importance vitale procède au cloisonnement de ses systèmes d'information d'importance vitale (SIIV) afin de limiter la propagation des attaques informatiques au sein de ses systèmes ou ses sous-systèmes. Il respecte les règles suivantes :

– chaque SIIV est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes de l'opérateur ou des systèmes tiers ;

– lorsqu'un SIIV est lui-même constitué de sous-systèmes, ceux-ci sont cloisonnés entre eux physiquement ou logiquement. Un sous-système peut être constitué pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIIV ou encore pour isoler des ressources d'un SIIV nécessitant un même besoin de sécurité ;

– seules les interconnexions strictement nécessaires au bon fonctionnement et à la sécurité d'un SIIV sont mises en place entre le SIIV et les autres systèmes ou entre les sous-systèmes du SIIV.

L'opérateur décrit dans le dossier d'homologation de chaque SIIV les mécanismes de cloisonnement qu'il met en place.

17. **Règle relative au filtrage**

L'opérateur d'importance vitale met en place des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information d'importance vitale (SIIV) afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques. Il respecte les règles suivantes :

– l'opérateur définit les règles de filtrage des flux de données (filtrage sur adresse réseau, sur protocole, sur numéro de port, etc.) permettant de limiter autant que possible la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIIV ;

– les flux entrants et sortants des SIIV ainsi que les flux entre sous-systèmes des SIIV sont filtrés au niveau de leurs interconnexions de manière à ne permettre que la circulation des seuls flux strictement nécessaires au fonctionnement et à la sécurité des SIIV. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués ;

– l'opérateur établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées depuis moins d'un an. Cette liste précise pour chaque règle :

– le motif et la date de la mise en œuvre, de la modification ou de la suppression de la règle ;

– les modalités techniques de mise en œuvre de la règle.

L'opérateur décrit dans le dossier d'homologation de chaque SIIV les mécanismes de filtrage qu'il met en place.

18. **Règle relative aux accès à distance**

L'opérateur d'importance vitale protège les accès à ses systèmes d'information d'importance vitale (SIIV) effectués à travers des réseaux tiers. En particulier, lorsque l'opérateur ou un prestataire qu'il a mandaté à cet effet accède à un SIIV à travers un réseau tiers à ceux de l'opérateur ou du prestataire, l'opérateur applique ou fait appliquer à son prestataire les règles suivantes :

– l'accès au SIIV est protégé par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;

– le mécanisme d'authentification utilisé est renforcé en mettant en œuvre une authentification à double facteur (authentification basée à la fois sur un élément secret et un autre élément propre à l'utilisateur) ;

– les équipements utilisés pour accéder au SIIV sont gérés et configurés par l'opérateur ou, le cas échéant, par le prestataire. Les mémoires de masse de ces équipements sont en permanence protégées par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information.

19. **Règle relative à l'installation de services et d'équipements**

L'opérateur d'importance vitale respecte les règles suivantes lorsqu'il installe des services et des équipements sur ses systèmes d'information d'importance vitale (SIIV) :

– l'opérateur installe sur ses SIIV les seuls services et fonctionnalités qui sont indispensables au fonctionnement ou à la sécurité de ses SIIV. L'opérateur désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'opérateur le mentionne dans le dossier d'homologation du SIIV concerné en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre ;
– l'opérateur ne connecte à ses SIIV que des équipements, matériels périphériques et supports amovibles qu'il a dûment répertoriés et qui sont indispensables au fonctionnement ou à la sécurité de ses SIIV ;
– les supports amovibles inscriptibles connectés aux SIIV sont utilisés exclusivement pour les besoins de ces SIIV ;
– l'opérateur procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de code malveillant. L'opérateur met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de code malveillant provenant de ces supports.

20. **Règle relative aux indicateurs**

L'opérateur d'importance vitale évalue, pour chaque système d'information d'importance vitale (SIIV), les indicateurs suivants :

– des indicateurs relatifs au maintien en conditions de sécurité des ressources :
– le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
– le pourcentage de serveurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
– le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas mises à jour ou corrigées du point de vue de la sécurité depuis au moins 15 jours à compter de la disponibilité des versions mises à jour ;
– le pourcentage de serveurs dont les ressources systèmes ne sont pas mises à jour ou corrigées du point de vue de la sécurité depuis au moins 15 jours à compter de la disponibilité des versions mises à jour ;
– des indicateurs relatifs aux droits d'accès des utilisateurs et à l'authentification des accès aux ressources :
  – le pourcentage d'utilisateurs accédant au SIIV au moyen de comptes partagés ;
  – le pourcentage d'utilisateurs accédant au SIIV au moyen de comptes privilégiés ;
  – le pourcentage de ressources dont les éléments secrets d'authentification ne peuvent pas être modifiés par l'opérateur ;
  – des indicateurs relatifs à l'administration des ressources :
  – le pourcentage de ressources administrées dont l'administration est effectuée à partir d'un compte non spécifique d'administration ;
  – le pourcentage de ressources administrées dont l'administration ne peut pas être effectuée au travers d'une liaison réseau physique ou d'une interface d'administration physique ;
  – le pourcentage de ressources administrées dont les flux d'administration ne peuvent pas être protégés par des mécanismes de chiffrement et d'authentification lorsque ces flux ne circulent pas dans le système d'information d'administration.

L'opérateur précise pour chaque indicateur la méthode d'évaluation employée et, le cas échéant, la marge d'incertitude de son évaluation. Lorsqu'un indicateur évolue de façon significative par rapport à l'évaluation précédente, l'opérateur en précise les raisons.

Les indicateurs ainsi réunis sont des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.

L'opérateur communique, une fois par an, à l'Agence nationale de la sécurité des systèmes d'information, ces indicateurs mis à jour, selon le moyen approprié à la sensibilité des informations déclarées.