

L L E I

Loi 22/2022, du 9 juin, portant mesures pour la sécurité des réseaux et des systèmes d'information

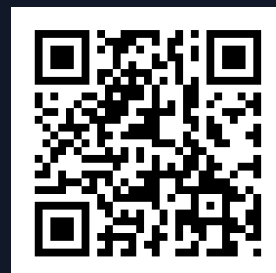
Texte en vigueur au 19/10/2026

Généré le 19/10/2026 à les 09:29

Données jusqu'au BOPA du 14/10/2026

Page en ligne : bopa.mca.ad/fr/llei/22-2022

Traduction réalisée par intelligence artificielle, à titre informatif. Seul le texte catalan publié au Butlletí Oficial del Principat d'Andorra fait foi. Les parties non traduites sont reproduites en catalan. Ce document ne constitue pas un conseil juridique ou fiscal.



Version à jour

Sommaire

TITRE I. DISPOSITIONS GÉNÉRALES

Article 1. Objet.....	4
Article 2. Champ d'application.....	4
Article 3. Définitions.....	5

TITRE II. CADRE STRATÉGIQUE ET INSTITUTIONNEL

Article 4. Cadre stratégique de sécurité des réseaux et des systèmes d'information.....	9
Article 5. Cadre national de gestion des crises de cybersécurité.....	11
Article 6. Autorités nationales compétentes.....	11
Article 7. Fonctions des autorités nationales compétentes.....	13

TITRE III. EN CE SENS, AVEC OU SANS LE SOUTIEN DU CSIRT-AD, LES AUTORITÉS NATIONALES COMPÉTENTES PEUVENT RÉALISER LES AC

TITRE IV. 8. ÉMETTRE DES AVIS SUR DES QUESTIONS RELATIVES À LA CYBERSÉCURITÉ. 9. DÉVELOPPER LES MEILLEURES PRATIQUES ET

Article 8. CSIRT-AD.....	14
Article 9. Fonctions du CSIRT-AD.....	14

CHAPITRE PREMIER. OBLIGATIONS DE CYBERSÉCURITÉ

Article 10. Obligation d'identification en tant qu'entité essentielle ou importante.....	15
Article 11. Identification des entités critiques.....	16
Article 12. Obligations de cybersécurité des entités essentielles et importantes.....	16
Article 13. Gestion des risques de cybersécurité.....	18
Article 14. Obligation de résoudre les incidents, d'information et de collaboration mutuelle.....	20
Article 15. Obligation de notification.....	20
Article 16. Notification volontaire.....	23
Article 17. Gouvernance.....	23
Article 18. Délégué à la Sécurité de l'Information.....	23
Article 19. Représentant dans la Principauté d'Andorre.....	25
Article 20. Utilisation de schémas de certification de cybersécurité.....	25
Article 21. Protection de l'auteur de la notification.....	26

CHAPITRE TROISIÈME. OBLIGATIONS DE SUPERVISION

Article 22. Supervision du respect des obligations de sécurité et des notifications d'incidents.....	26
Article 23. Supervision et exécution dans le cas des entités essentielles.....	27
Article 24.....	29

CHAPITRE QUATRIÈME. AUTRES OBLIGATIONS DES AUTORITÉS NATIONALES COMPÉTENTES ET DU CSIRT-AD

Article 25. Obligations des autorités nationales compétentes.....	30
Article 26. Obligations du.....	32
Article 27. Coopération nationale.....	33
Article 28. Coopération transfrontalière.....	33
Article 29. Confidentialité des informations sensibles.....	34
Article 30. Pouvoir de sanction.....	34
Article 31. Responsables des infractions.....	34
Article 32. Dossier de sanction.....	34
Article 33. Infractions.....	35
Article 34. Classification des infractions.....	35
Article 35. Infractions entraînant une violation de la sécurité des données personnelles.....	36
Article 36. Sanctions.....	36
Article 37. Graduation des sanctions.....	37
Article 38. Proportionnalité des sanctions.....	37
Article 39. Concours d'infractions.....	38
Article 40. Prescription des infractions.....	38

Article 41. P rescription des sanctions.....38

Disposition additionnelle première. Mission confiée au Gouvernement 39

Disposition finale première. Modification de la Loi 31/2021 , du 22 novembre, portant texte consolidé qualifiée de
sécurité publique 39

Disposition finale deuxième. Développement réglementaire.....39

Disposition finale troisième. Texte consolidé 39

Disposition finale quatrième. Entrée en vigueur.....40

Annexe 1. Entités essentielles 40

Annexe 2. Entités importantes.....42

Titre I. Dispositions générales

Article 1. Objet

1. La présente Loi a pour objet de réglementer le renforcement de la résilience des entités critiques et la sécurité des réseaux et des systèmes d'information utilisés pour la prestation de services essentiels et importants dans la Principauté d'Andorre.
2. Pour atteindre son objet, la présente Loi établit principalement :
 - a) Les conditions requises pour la protection des services essentiels et des services importants, les obligations de gestion des risques et des incidents de cybersécurité incombant aux entités prestataires de ces services, et les mécanismes de contrôle de leur respect, y compris un système de notification des incidents ;
 - b) L'obligation pour les autorités nationale compétentes d'identifier les entités critiques et les entités qui doivent être traitées comme équivalentes à des entités critiques sous certains aspects, parce que, sans fournir elles-mêmes les services essentiels, elles peuvent toutefois avoir un impact sur ceux-ci ;
 - c) L'obligation pour les entités critiques d'adopter certaines mesures, établies par voie réglementaire, destinées à garantir la prestation de services essentiels ;
 - d) Un cadre pour l'élaboration d'un catalogue national des entités essentielles pour la sécurité des réseaux et des systèmes d'information ; et
 - e) Un cadre institutionnel pour l'application de la Stratégie nationale de sécurité des réseaux et des systèmes d'information.
3. Les dispositions de la présente Loi s'entendent sans préjudice des actions que peuvent entreprendre les autorités publiques compétentes pour sauvegarder et garantir la sécurité nationale et les fonctions essentielles, pour protéger les informations réservées de l'État ou dont la divulgation serait contraire aux intérêts essentiels de la Principauté d'Andorre, ou pour le maintien de l'ordre public, la détection, l'investigation et la poursuite des infractions pénales, et le jugement de leurs auteurs.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 2. Champ d'application

1. La présente Loi s'applique aux entités publiques et privées prévues dans le cadre des entités essentielles et importantes conformément à leur définition à l'article 3, qui emploient 50 personnes ou plus ou dont le chiffre d'affaires annuel ou le bilan annuel total dépasse dix millions d'euros.
2. En outre, la présente Loi s'applique aux entités essentielles et importantes indépendamment de leur taille et de leur chiffre d'affaires annuel ou de leur bilan annuel total, lorsque :
 - a) les services sont fournis par l'un des types d'entités suivants relevant du secteur des infrastructures numériques de l'Annexe I : i. réseaux publics de communications électroniques ou services de communications électroniques accessibles au public, ii. prestataires de services de confiance, et iii. registres de noms de domaine de premier niveau et fournisseurs de services de système de noms de domaine (DNS).

- b) l'entité est une entité de l'administration publique telle que définie à l'article 3.12 ;
 - c) l'entité est l'unique prestataire d'un service dans la Principauté d'Andorre ;
 - d) une perturbation éventuelle du service fourni par l'entité pourrait avoir des répercussions sur la sécurité publique, l'ordre public ou la santé publique ;
 - e) une perturbation éventuelle du service fourni par l'entité pourrait induire des risques systémiques, en particulier pour les secteurs dans lesquels une telle perturbation pourrait avoir des répercussions de nature transfrontière ;
 - f) l'entité est critique en raison de son importance spécifique au niveau national ou communal pour le secteur ou le type de service concerné ou pour d'autres secteurs interdépendants dans la Principauté d'Andorre ; ou
 - g) l'entité est identifiée comme entité critique ou comme une entité équivalente à une entité critique par voie réglementaire.
3. Les règlements et les autres normes et actes juridiques éventuels de nature sectorielle en rapport avec la présente Loi qui prévoient des dispositions relatives à la gestion des risques liés aux technologies de l'information et de la communication (TIC), à la gestion ou à la notification des incidents liés aux TIC, aux tests de résilience opérationnelle numérique, aux mécanismes d'échange d'informations et au risque lié aux tiers en matière de TIC, et qui ont un effet au moins équivalent à celui des obligations établies dans la présente Loi, s'appliquent en priorité aux entités essentielles et importantes relevant du champ d'application desdits règlements, normes et actes juridiques.
4. Les dispositions du paragraphe précédent s'entendent sans préjudice de l'obligation de notification des incidents établie à l'article 15, dans la mesure où elle n'est pas incompatible avec la réglementation sectorielle concernée.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 3. Définitions

Aux fins de la présente Loi, on entend par :

1. AFA : Autorité financière andorrane.
2. ANC-AD : Agence nationale de cybersécurité de la Principauté d'Andorre.
3. APDA : Agence andorrane de protection des données.
4. Évaluation des risques : une méthodologie permettant de déterminer la nature et la portée d'un risque au moyen de l'analyse des menaces et des dangers potentiels, et de l'évaluation des conditions de vulnérabilité existantes qui pourraient perturber les opérations de l'entité critique.
5. Cybermenaces : une circonstance, un événement ou une action potentielle susceptible d'endommager, d'interrompre ou d'affecter de manière préjudiciable les réseaux et les systèmes d'information, ainsi que leurs utilisateurs et d'autres parties intéressées.
6. Cybersécurité : les activités nécessaires à la protection des réseaux et des systèmes d'information, de leurs utilisateurs et d'autres personnes touchées par les cybermenaces.
7. CSIRT : centre de réponse aux incidents de sécurité des réseaux et des systèmes d'information.

8. CSIRT-AD : CSIRT de référence de la Principauté d'Andorre.
9. DNS, ou Système de noms de domaine : un système de nommage distribué de manière hiérarchique qui permet aux utilisateurs finaux d'accéder aux services et aux ressources d'Internet.
10. Entité : toute personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu d'établissement et qui, agissant en son nom propre, peut exercer des droits et être soumise à des obligations.
11. Entité critique : une entité qui fournit un ou plusieurs services essentiels dont la prestation dépend d'une ou de plusieurs infrastructures critiques situées dans la Principauté d'Andorre.
12. Entité de l'administration publique : une entité de la Principauté d'Andorre qui remplit les critères suivants :
 - a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial ;
 - b) elle est dotée de la personnalité juridique ;
 - c) elle est majoritairement financée par le Gouvernement d'Andorre, les Comuns ou des entités de droit public ; ou bien sa gestion est soumise à un contrôle de la part de ces administrations ou entités ; ou ses organes d'administration, de direction ou de surveillance sont composés de membres dont plus de la moitié sont nommés par le Gouvernement d'Andorre, les Comuns ou des entités de droit public ; et.
 - d) elle fournit un service public. Sont exclues les entités de l'administration publique qui exercent des activités dans les domaines de la sécurité publique, de la police, de la défense ou de la sécurité nationale.
13. Entité de registre des noms de domaine de premier niveau : une entité à laquelle a été délégué un domaine de premier niveau spécifique et qui est chargée d'administrer ce domaine, y compris l'enregistrement des noms de domaine relevant du premier niveau et le fonctionnement technique du domaine de ce niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau entre les serveurs de noms.
14. Entité équivalente à une entité critique : toute entité qui, sans être critique, gère une ou plusieurs infrastructures critiques situées dans la Principauté d'Andorre.
15. Entité essentielle : toute entité de l'administration publique ou privée qui offre un service essentiel conformément à la définition du paragraphe 35.
16. Entité importante : toute entité de l'administration publique ou privée qui offre un service important conformément à la définition du paragraphe 36.
17. Stratégie nationale de cybersécurité : cadre cohérent de la Principauté d'Andorre qui établit des priorités et des objectifs stratégiques en matière de sécurité des réseaux et des systèmes d'information dans le pays.
18. Gestion des incidents : ensemble de mesures et de procédures destinées à détecter, analyser et limiter un incident et à y répondre.
19. Gestion des risques : processus de planification de la gestion des risques, et ensemble d'activités visant à identifier, analyser, traiter, surveiller et contrôler les risques.

20. Incident : tout événement susceptible de perturber ou qui perturbe les opérations d'une entité, ou qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées, ou des services correspondants offerts par des réseaux et des systèmes d'information ou accessibles par leur intermédiaire.
21. Infrastructure : un actif, un système ou une partie de celui-ci, nécessaire à la prestation d'un service essentiel.
22. Infrastructures critiques : infrastructures qui sont indispensables et ne permettent pas de solutions alternatives, de sorte que leur perturbation ou leur destruction aurait des effets préjudiciables significatifs sur la prestation d'un ou de plusieurs services essentiels.
23. Place de marché en ligne : un service numérique qui permet aux consommateurs de conclure des contrats à distance au moyen d'une interface en ligne.
24. Moteur de recherche en ligne : un service numérique qui permet aux utilisateurs de saisir des requêtes afin d'effectuer des recherches, en principe, sur tous les sites web, ou sur des sites web dans une langue donnée, au moyen d'une requête portant sur un sujet quelconque sous la forme d'un mot-clé, d'une requête vocale, d'une phrase ou d'un autre type d'entrée et qui, en réponse, affiche des résultats dans tout format dans lequel peuvent être trouvées des informations en rapport avec le contenu demandé.
25. Organe de direction : l'organe ou les organes d'administration de l'entité nommés conformément au droit national, habilités à fixer la stratégie, les objectifs et l'orientation générale de l'administration de cette entité, ou les personnes équivalentes qui dirigent effectivement l'entité ou exercent des fonctions clés conformément à la législation andorrane.
26. Plateforme de services de réseaux sociaux : une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur de multiples appareils et, en particulier, au moyen de discussions en ligne, de publications, de vidéos et de recommandations ;
27. Fournisseur de services DNS : une entité qui fournit des services de résolution récursive de noms de domaine aux utilisateurs finaux d'Internet et à d'autres fournisseurs de services DNS, ou une entité qui fournit une résolution de noms de domaine faisant autorité en tant que service pouvant être obtenu par des entités essentielles ou importantes auprès de tiers.
28. Quasi-incident : tout événement qui possède le potentiel de produire un incident et qui ne parvient pas à le produire, que ce soit par hasard ou grâce à une intervention opportune.
29. Résilience : la capacité de prévenir un incident qui perturbe ou est susceptible de perturber les opérations d'une entité critique, d'y résister, de l'atténuer, de l'absorber, de s'y adapter et de s'en rétablir.
30. Risque : toute circonstance ou tout fait susceptible d'avoir un effet préjudiciable potentiel sur la résilience des entités critiques ;
31. Sécurité des réseaux et des systèmes d'information : la capacité des réseaux et des systèmes d'information de résister, avec un niveau de fiabilité déterminé, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées, ou des services correspondants offerts par lesdits réseaux et systèmes d'information ou accessibles par leur intermédiaire.

32. Service d'informatique en nuage : un service numérique qui permet l'administration à la demande et un large accès à distance à un ensemble modulable et élastique de ressources informatiques distribuées pouvant être partagées.
33. Service de centre de données : un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, à l'interconnexion et à l'exploitation centralisés des technologies de l'information et des équipements de réseau fournissant des services de stockage, de traitement et de transport de données, ainsi que l'ensemble des installations et infrastructures nécessaires à la distribution de l'énergie et au contrôle environnemental.
34. Service numérique : tout service de la société de l'information, c'est-à-dire tout service fourni normalement contre rémunération, à distance, à la demande individuelle d'un destinataire de services, et envoyé à la source et reçu par le destinataire au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par tout autre moyen électromagnétique.
35. Service essentiel : service offert par une entité dont la typologie relève de celle des entités essentielles prévues à l'Annexe I, que les autorités nationales compétentes désignent comme tel conformément à l'article 6.4.b), en ce qu'il est nécessaire au maintien des fonctions sociales de base, de la santé, de la sécurité, du bien-être social et économique des citoyens, ou au fonctionnement efficace des institutions de l'État et des administrations publiques, qui dépend pour sa fourniture de réseaux et de systèmes d'information, et dont la continuité des prestations peut être gravement affectée en cas de cyberincidents et, par conséquent, causer un grave préjudice social et économique à la Principauté d'Andorre.
36. Service important : service offert par une entité dont la typologie relève de celle d'entité importante à l'Annexe II, que les autorités nationales compétentes désignent comme tel conformément à l'article 6.4.b), en ce qu'il est nécessaire au maintien des fonctions sociales de base, de la santé, de la sécurité, du bien-être social et économique des citoyens, ou au fonctionnement efficace des institutions de l'État et des administrations publiques, qui dépend pour sa fourniture de réseaux et de systèmes d'information, et dont la continuité des prestations peut être gravement affectée en cas de cyberincidents et, par conséquent, causer un grave préjudice social et économique à la Principauté d'Andorre,
37. Vulnérabilité : déficience, susceptibilité ou défaillance d'un actif, d'un système, d'un processus ou d'un contrôle qui peut être exploitée par une ou plusieurs cybermenaces.
38. Réseau de diffusion de contenu : un réseau de serveurs répartis géographiquement aux fins de garantir une haute disponibilité, l'accessibilité ou la distribution rapide de contenus et de services numériques aux utilisateurs d'Internet pour le compte des fournisseurs de contenus et de services.
39. Réseaux et systèmes d'information :
- a) Réseau de communications électroniques, consistant en des systèmes de transmission et, le cas échéant, des équipements de commutation ou de routage et d'autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par ondes hertziennes, par moyens optiques ou par d'autres moyens électromagnétiques, y compris les réseaux satellitaires, les réseaux terrestres fixes (à commutation de circuits et de paquets, y compris Internet) et mobiles, les systèmes utilisant le

réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle, et les réseaux câblés de télévision, quel que soit le type d'information acheminée ;

- b) Tout dispositif ou groupe de dispositifs interconnectés ou liés entre eux, dont un ou plusieurs assurent, au moyen d'un logiciel, le traitement automatisé de données numériques ; ou
- c) Les données numériques stockées, traitées, récupérées ou transmises au moyen des éléments prévus aux lettres précédentes, en vue de leur fonctionnement, de leur utilisation, de leur protection et de leur maintenance.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Titre II. Cadre stratégique et institutionnel

Article 4. Cadre stratégique de sécurité des réseaux et des systèmes d'information

1. La Stratégie nationale de cybersécurité de la Principauté d'Andorre comprend les objectifs stratégiques et les mesures politiques et normatives nécessaires pour atteindre et maintenir un niveau élevé de sécurité des réseaux et des systèmes d'information, couvrant les secteurs exploités par les entités essentielles et importantes dans les termes définis par la présente Loi, et englobe, à titre indicatif et non limitatif :
 - a) Une définition des objectifs et des priorités de la Stratégie nationale de cybersécurité de la Principauté d'Andorre.
 - b) Un cadre de gouvernance pour atteindre ces objectifs et priorités, y compris les politiques visées au paragraphe 2 et les fonctions et responsabilités des administrations publiques et des entités de l'administration publique ainsi que d'autres acteurs pertinents.
 - c) Une évaluation visant à déterminer les actifs pertinents et les risques de cybersécurité.
 - d) Une détermination des mesures visant à garantir la préparation et la réaction aux incidents ainsi que le rétablissement après ceux-ci, y compris la coopération entre les secteurs public et privé.
 - e) Une liste des différents acteurs et autorités participant à la mise en œuvre de la Stratégie nationale de cybersécurité de la Principauté d'Andorre.
 - f) Un cadre politique pour une coordination renforcée entre les autorités compétentes en vertu de la présente Loi aux fins de l'échange d'informations sur les incidents et les cybermenaces et de l'exercice des missions de supervision et de sanction.
 - g) Une stratégie visant à renforcer la résilience des entités critiques, comprenant au minimum : i. Des objectifs stratégiques et des priorités afin d'améliorer la résilience générale des entités critiques, compte tenu des interdépendances transfrontalières et intersectorielles. ii. Un cadre de gouvernance pour atteindre les objectifs stratégiques et les priorités, y compris une description des rôles et des responsabilités des autorités nationales compétentes désignées par la présente Loi, des entités critiques et des autres parties concernées par la mise en œuvre de la stratégie. iii. Une description des mesures nécessaires pour améliorer la résilience générale des entités critiques, y compris une évaluation du risque national, l'identification des entités critiques et des entités équivalentes à des enti-

tés critiques et les mesures de soutien aux entités critiques ; et iv. Un cadre de politiques pour une coordination améliorée entre les autorités nationales compétentes désignées par la présente Loi aux fins de l'échange d'informations sur les incidents et les cybermenaces et de l'exercice des missions de supervision.

2. Dans le cadre de la Stratégie nationale de cybersécurité de la Principauté d'Andorre, sont élaborés et adoptés par voie réglementaire :

- a) Un Schéma national de sécurité constitué des principes de base et des conditions requises minimales nécessaires à une protection adéquate des informations traitées et des services fournis par les entités essentielles et les entités importantes, ainsi que par les entités qui leur fournissent des services ou des solutions pour leurs services essentiels ou importants et leurs chaînes d'approvisionnement respectives, dans le but d'assurer l'accès, la confidentialité, l'intégrité, la traçabilité, l'authenticité, la disponibilité et la conservation des données, des informations et des services utilisés sur des supports électroniques qu'elles gèrent pour la fourniture des services essentiels ou importants, et sans préjudice du fait qu'il puisse s'avérer nécessaire de compléter les mesures de sécurité prévues par ce schéma par d'autres mesures spécifiques pouvant découler des engagements internationaux contractés par la Principauté d'Andorre ou de son appartenance à des organismes ou forums internationaux en la matière.

Ce Schéma national de sécurité peut être étendu à toutes les entités de l'administration publique et contient, au minimum : i. Une politique visant à traiter la cybersécurité dans la chaîne d'approvisionnement des produits et services TIC utilisés par les entités essentielles ou les entités importantes pour la fourniture de leurs services ; ii.

Des lignes directrices relatives à l'inclusion et à la spécification des conditions requises en matière de cybersécurité applicables aux produits et services TIC dans la commande publique ; iii.

Une politique visant à promouvoir et à faciliter une divulgation coordonnée des vulnérabilités ; iv.

Une politique visant à maintenir la disponibilité générale et l'intégrité du noyau public de l'Internet ouvert ; v. Une politique relative à la promotion et au développement des capacités de cybersécurité, y compris la sensibilisation et les initiatives de recherche et de développement ; vi.

Une politique destinée à soutenir les institutions universitaires et de recherche afin qu'elles développent des outils de cybersécurité et des infrastructures de réseau sécurisées ; vii.

Les politiques, les procédures pertinentes et les outils appropriés de partage d'informations afin de faciliter et de promouvoir l'échange volontaire d'informations sur la cybersécurité entre les entreprises ; et viii.

Une politique englobant les besoins spécifiques des petites et moyennes entreprises, en particulier de celles qui sont exclues du champ d'application de la présente Loi, en ce qui concerne les orientations et le soutien visant à améliorer leur résilience face aux menaces de cybersécurité.

- b) Un Règlement des infrastructures critiques pour la protection et le renforcement de la résilience des infrastructures critiques, qui contient, au minimum : i. Des procédures d'identification et de désignation des infrastructures critiques pour la Principauté d'Andorre ; ii. Les

conditions de création d'un Catalogue national des infrastructures critiques, qui doit rassembler toutes les données et l'évaluation de la criticité desdites infrastructures et qui sera utilisé comme base pour planifier les actions nécessaires en matière de sécurité et de protection de celles-ci, en s'alimentant des apports des opérateurs eux-mêmes ; iii. La réglementation des instruments de planification pour la protection des infrastructures critiques des entités essentielles et des entités importantes ; iv. Les obligations des entités critiques, y compris les conditions requises de sécurité des communications, afin d'accroître leur résilience et d'améliorer leur capacité à fournir leurs services à la Principauté d'Andorre ; et v. Les règles relatives à la supervision des entités critiques et à l'application d'obligations à celles-ci.

3. La Stratégie nationale de cybersécurité de la Principauté d'Andorre doit faire l'objet d'une révision et d'une évaluation au moins tous les quatre ans, en fonction des indicateurs clés de performance, et doit en tout état de cause être modifiée lorsque cela est nécessaire. La consultation des secteurs pertinents représentés dans les différents comités et commissions structurés sous l'Agence nationale de cybersécurité (ANC-AD) doit être garantie.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 5. Cadre national de gestion des crises de cybersécurité

1. L'ANC-AD est responsable de la gestion des incidents et des crises à grande échelle, pour lesquels :
 - a) Elle détermine les capacités, les actifs et les procédures pouvant être déployés en cas de survenance d'une crise aux fins de la présente Loi ; et
 - b) Elle élabore un Plan national de réponse aux incidents et crises de cybersécurité, dans un délai maximal de neuf mois à compter de l'entrée en vigueur de la présente Loi, qui fixe les objectifs et les modalités de la gestion des incidents et des crises de cybersécurité, et qui doit contenir au moins les aspects suivants : i. Les objectifs des mesures et activités nationales en matière de préparation ; ii. Les tâches et responsabilités des autorités nationales compétentes conformément aux dispositions de la présente Loi ; iii. Les procédures de gestion des crises et les canaux d'échange d'informations ; iv. Les mesures de préparation, y compris les exercices et les activités de formation ; v. Les parties intéressées pertinentes, tant publiques que privées, et l'infrastructure concernée ; et vi. Les procédures et mécanismes nationaux entre l'ANC-AD, le CSIRT-AD et d'autres autorités ou organismes nationaux pertinents pour garantir la participation effective de la Principauté d'Andorre à la gestion coordonnée des incidents et crises de cybersécurité. Chapitre II. Cadre institutionnel

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 6. Autorités nationales compétentes

1. L'ANC-AD est l'autorité nationale compétente chargée de la cybersécurité et des tâches de supervision visées au chapitre troisième du Titre III pour les réseaux et les systèmes d'information couvrant les secteurs mentionnés aux paragraphes 1, 2, 5, 6, 7 et 8 de l'Annexe I, ainsi que pour toutes les entités importantes pour lesquelles l'AFA n'est pas l'autorité nationale compétente.

2. L'AFA, en coordination avec l'ANC-AD, est l'autorité nationale compétente chargée de la cybersécurité et des tâches de supervision visées au chapitre troisième du Titre III pour les réseaux et les systèmes d'information couvrant les secteurs des entités financières et du marché financier tels que définis aux paragraphes 3 et 4 de l'Annexe I, ainsi que pour les services fournis par les entités placées sous la supervision de l'AFA.
3. L'ANC-AD agit en tant que point de contact unique en matière de cybersécurité pour la Principauté d'Andorre (Point de Contact National Unique), et à ce titre est l'autorité nationale compétente qui exerce la fonction de liaison afin de garantir la coopération transfrontalière avec les autorités compétentes en matière de cybersécurité d'autres pays, de garantir la coopération intersectorielle entre l'AFA et l'ANC-AD en ce qui concerne les dispositions de la présente Loi, ainsi que de garantir la coopération entre le CSIRT-AD et les autres pays, y compris le réseau des CSIRT de l'Union européenne.
4. L'ANC-AD, avec la collaboration de l'AFA en ce qui concerne son domaine de compétence conformément aux dispositions de la présente Loi :
 - a) Coordonne la création et le maintien du cadre stratégique de sécurité des réseaux et des systèmes d'information décrit à l'article 4.
 - b) Établit une liste des services essentiels et des services importants dans les secteurs visés à l'Annexe I et à l'Annexe II. Cette liste doit être établie dans un délai maximal de six mois après l'entrée en vigueur de la présente Loi. Par la suite, lorsque cela est nécessaire, et au moins une première fois dans un délai maximal de dix-huit mois après l'entrée en vigueur de la présente Loi et, à partir de ce moment, tous les quatre ans et chaque fois que l'ANC-AD met à jour la liste, elle procède à une évaluation de tous les risques pertinents susceptibles d'affecter la fourniture de ces services essentiels, afin d'identifier les entités critiques et les entités équivalentes à des entités critiques et de les aider à prendre des mesures conformément aux dispositions de l'article 12. L'évaluation des risques : i. Doit tenir compte de tous les risques naturels et d'origine humaine, y compris les accidents, les catastrophes naturelles, les urgences de santé publique et les menaces antagonistes, y compris les infractions terroristes. ii. Les éléments pertinents de l'évaluation des risques doivent être mis à la disposition des entités critiques identifiées conformément aux dispositions de l'article 11, afin de les aider à réaliser leur évaluation des risques conformément aux dispositions de l'article 13 et à prendre des mesures pour garantir leur résilience conformément aux dispositions de l'article 12.
 - c) Apporte son soutien aux entités relevant du champ d'application de la présente Loi afin d'améliorer leur cybersécurité et leur résilience. Ce soutien peut comprendre, à titre informatif et non limitatif : i. L'élaboration de supports et de méthodologies d'orientation ; ii. Le soutien à l'organisation d'exercices visant à vérifier leur sécurité et leur résilience ; iii. La fourniture de formations à leur personnel ; et iv. La mise en place d'outils destinés à soutenir l'échange volontaire d'informations entre entités et à résoudre des questions relatives à la présente Loi.
 - d) Adopte des actes d'exécution afin d'établir les spécifications techniques et méthodologiques nécessaires relatives à l'application des mesures mentionnées à l'article 12.2.
 - e) Établit des procédures pour la délivrance, la révision périodique et le retrait des certifications, labels et marques attestant le respect des obligations de sécurité des réseaux et des systèmes d'information.

- f) Établit des procédures et des structures pour traiter les réclamations relatives aux infractions à la certification ou à la manière dont une entité applique ou a appliqué la certification, et pour rendre ces procédures et structures transparentes pour le public.
5. L'ANC-AD, avec la collaboration de l'AFA et du CSIRT-AD, est habilitée à adopter des actes délégués établissant des règles détaillées précisant tout ou partie des mesures à prendre dans la mesure nécessaire à l'application efficace et cohérente des objectifs de la présente Loi, compte tenu de toute évolution pertinente des risques, de la technologie ou de la fourniture des services concernés par la présente Loi, ainsi que de toute spécificité liée aux secteurs et types d'entités de l'Annexe I et de l'Annexe II.
6. Le Gouvernement d'Andorre doit veiller à ce que les autorités nationales compétentes disposent des ressources adéquates pour pouvoir exercer de manière effective et efficiente leurs fonctions afin de pouvoir atteindre les objectifs de la présente Loi.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 7. Fonctions des autorités nationales compétentes

Les autorités nationales compétentes exercent les fonctions suivantes :

1. Identifier, en collaboration avec le CSIRT-AD, les services essentiels et importants, les entités critiques et les entités équivalentes à des entités critiques.
2. Superviser le respect, par les entités essentielles ou importantes, des obligations déterminées conformément aux dispositions du chapitre troisième du

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Titre III. En ce sens, avec ou sans le soutien du CSIRT-AD, les autorités nationales compétentes peuvent réaliser les actions d'inspection nécessaires au bon exercice de leurs fonctions de contrôle. 3. Analyser les notifications qu'elles reçoivent par l'intermédiaire du CSIRT-AD concernant les incidents notables qui surviennent dans le cadre de la présente Loi. 4. Informer, le cas échéant, publiquement sur certains incidents, lorsque la diffusion de ces informations est nécessaire pour prévenir un incident ou gérer un incident qui s'est déjà produit. 5. Examiner la déclaration d'applicabilité des mesures de sécurité initiale visée à l'article 12, ainsi que ses modifications successives. 6. Statuer sur les demandes d'informations conformément à l'article 12.2.e), concernant le personnel ou les candidats à des postes de personnel exerçant des fonctions critiques. 7. Exercer le pouvoir de sanction dans les cas prévus par la présente Loi, en vertu des dispositions de son

Titre IV. 8. Émettre des avis sur des questions relatives à la cybersécurité. 9. Développer les meilleures pratiques et méthodologies de mise en œuvre des obligations visées par la présente Loi. 10. Développer des activités et des exercices de formation transfrontaliers pour vérifier la cybersécurité des services essentiels et la résilience des entités critiques. 11. Délivrer, après consultation préalable du CSIRT-AD, aux entités essentielles ou importantes, des certificats attestant le respect des obligations de sécurité des réseaux et des systèmes d'information.

Article 8. CSIRT-AD

1. Le CSIRT-AD est l'équipe de référence de réponse aux incidents de sécurité des réseaux et des systèmes d'information des secteurs, sous-secteurs ou entités figurant à l'Annexe I et à l'Annexe II.
2. L'ANC-AD doit veiller à ce que le CSIRT-AD dispose des ressources adéquates pour pouvoir exercer de manière effective et efficiente les fonctions que lui attribuent la présente Loi, son Règlement de création et toute autre réglementation éventuelle.
3. De même, l'ANC-AD doit veiller à ce que le CSIRT-AD ait à sa disposition une infrastructure de communication et d'information adéquate, sécurisée et résiliente pour faciliter l'échange d'informations avec les entités essentielles et importantes et les autres parties intéressées pertinentes.

Redacció vigent des del 23/06/2024 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 9. Fonctions du CSIRT-AD

1. Le CSIRT-AD a pour principales fonctions de :

- a) Coopérer avec l'ANC-AD pour tout ce que celle-ci lui demande en relation avec la présente Loi.
 - b) Surveiller les cybermenaces, les vulnérabilités et les incidents à l'échelle nationale.
 - c) Diffuser des alertes imminentes, des avis et des informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes et des autres parties intéressées concernées.
 - d) Fournir aux entités qui notifient des incidents des informations pertinentes sur le suivi de la notification concernée, y compris des informations susceptibles de soutenir la réponse effective de l'entité à l'incident.
 - e) Répondre aux incidents.
 - f) Notifier à l'ANC-AD les incidents notables qui surviennent dans le cadre de la présente Loi.
 - g) Effectuer des analyses dynamiques des risques et des incidents et de connaissance de la situation en matière de cybersécurité.
 - h) Réaliser, à la demande d'entités, des analyses proactives de la sécurité des infrastructures critiques et des réseaux et systèmes d'information utilisés dans la fourniture des services essentiels ou susceptibles d'affecter des services essentiels pour la Principauté d'Andorre ou d'autres pays.
 - i) Se coordonner avec les organismes compétents au moyen des protocoles d'action pour l'application de la présente Loi qui, le cas échéant, peuvent être développés par voie réglementaire.
 - j) Élaborer et encourager l'adoption et l'utilisation de pratiques communes ou normalisées, de systèmes de classification et de taxonomies relatifs aux : i. Procédures de gestion des incidents ; ii. Gestion des crises de cybersécurité ; et iii. Divulgarion des vulnérabilités.
- III. Obligations

Redacció vigent des del 23/06/2024 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Chapitre premier. Obligations de cybersécurité

Article 10. Obligation d'identification en tant qu'entité essentielle ou importante

1. Les entités qui, conformément aux définitions figurant à l'article 3, sont considérées comme essentielles ou importantes, relèvent du champ d'application décrit à l'article 2 et disposent d'un établissement dans la Principauté d'Andorre ou d'un représentant conformément aux dispositions de l'article 19, transmettent les informations suivantes à leurs autorités nationales compétentes respectives au plus tard six mois à compter de la date de publication au Bulletin officiel de la Principauté d'Andorre de la liste des services essentiels et importants établie à l'article 6.4.b) :
- a) Le nom de l'entité et, le cas échéant, de son représentant ;
 - b) L'adresse de son établissement principal et de ses autres établissements légaux dans la Principauté d'Andorre ou, si elle n'est pas établie dans la Principauté d'Andorre, de son représentant désigné en vertu des dispositions de l'article 19 ; et

- c) Les coordonnées actualisées, en particulier les adresses de courrier électronique et les numéros de téléphone des entités.
2. Les entités visées au paragraphe précédent notifient à leurs autorités nationales compétentes respectives toute modification des informations transmises conformément audit paragraphe sans délai et, en tout état de cause, dans un délai maximal de trois mois à compter de la date à laquelle la modification intervient.
3. Lorsque, outre la Principauté d'Andorre, une entité visée au paragraphe 1 a son établissement principal dans d'autres pays, l'ANC-AD informe également les autorités compétentes de ces pays de la qualité d'entité essentielle ou importante pour la Principauté d'Andorre que possède cette entité.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 11. Identification des entités critiques

1. Dans un délai maximal de six mois à compter de la conclusion de l'évaluation des risques visée à l'article 6.4.b), les autorités nationales compétentes doivent avoir identifié les entités critiques et les entités équivalentes à des entités critiques pour chaque secteur et sous-secteur visé à l'Annexe I. Les autorités nationales compétentes doivent réviser et, le cas échéant, mettre à jour cette liste d'entités critiques et équivalentes une première fois au moins dans un délai maximal de dix-huit mois après l'entrée en vigueur de la présente Loi et, en tout état de cause, au moins tous les quatre ans.
2. Lorsqu'elles identifient des entités critiques et des entités équivalentes à des entités critiques conformément au paragraphe 1, les autorités nationales compétentes doivent tenir compte des résultats de leur évaluation des risques susceptibles d'affecter les services essentiels relevant de leur compétence, conformément aux dispositions de l'article 6, et appliquer les critères qui identifient une entité comme entité critique conformément à sa définition.
3. L'ANC-AD, avec la collaboration de l'AFA en ce qui concerne son domaine de compétence conformément aux dispositions de la présente Loi, doit établir une liste des entités identifiées comme critiques ou équivalentes à des entités critiques et s'assurer que leur identification comme entités critiques ou équivalentes à des entités critiques soit notifiée à ces entités dans un délai d'un mois après cette identification, en les informant de leurs obligations conformément aux autres articles du présent chapitre et de la date à partir de laquelle leur sont applicables les dispositions établies par la présente Loi et par les règlements qui la développent, en ce qui concerne lesdites obligations.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 12. Obligations de cybersécurité des entités essentielles et importantes

1. Les entités essentielles et importantes soumises au champ d'application de la présente Loi doivent adopter des mesures techniques et organisationnelles résultant de la gestion des risques qui se posent en relation avec la sécurité des infrastructures critiques, ainsi que des réseaux et des systèmes d'information utilisés dans la prestation des services essentiels et importants, qu'il s'agisse d'infrastructures critiques, de réseaux et de systèmes propres ou de fournisseurs externes.

De même, elles doivent tenir compte, en particulier, de la dépendance des infrastructures critiques, des réseaux et des systèmes d'information à l'égard de la continuité des services ou des fournitures contractés par l'entité, ainsi que des interactions qu'elles réalisent avec des infrastructures, des réseaux et des systèmes d'information de tiers, et des risques découlant du traitement des données à caractère personnel, conformément aux dispositions de la réglementation andorrane en vigueur à tout moment en matière de protection des données à caractère personnel et, le cas échéant, de la réglementation de l'Union européenne en vigueur à tout moment en matière de protection des données à caractère personnel.

Sans préjudice de leur devoir de notifier les incidents conformément aux dispositions de l'article 15, les entités essentielles et importantes doivent prendre les mesures adéquates et proportionnées qui leur sont applicables conformément aux prévisions du Schéma national de sécurité auquel se réfère la présente Loi, sans préjudice de la possibilité de les compléter par des mesures issues d'autres normes reconnues au niveau international.

2. En outre, les entités critiques doivent prendre des mesures techniques et organisationnelles adéquates et proportionnées pour garantir la résilience de leurs infrastructures critiques, y compris les mesures nécessaires pour :
 - a) Éviter que des incidents ne se produisent, y compris au moyen de mesures de réduction du risque de catastrophes et d'adaptation climatique ;
 - b) Garantir une protection physique adéquate des zones, des installations et des autres infrastructures sensibles, y compris les clôtures, les barrières, les outils et les procédures de contrôle périmétrique, ainsi que les équipements de détection et les contrôles d'accès ;
 - c) Résister aux conséquences des incidents et les atténuer, y compris par la mise en œuvre de procédures et de protocoles de gestion des risques et des crises et de procédures d'alerte ;
 - d) Se rétablir à la suite des incidents, y compris par des mesures de continuité des activités et l'identification de chaînes d'approvisionnement alternatives ;
 - e) Garantir une gestion adéquate de la sécurité des employés, y compris l'établissement de catégories de personnel exerçant des fonctions critiques en raison de leurs droits d'accès à des zones, des installations et d'autres infrastructures sensibles et à des informations sensibles, au sujet desquelles il convient de présenter à l'autorité nationale compétente un rapport comprenant : i. L'identité de la personne, établie sur la base de preuves documentaires ; ii. Tout antécédent pénal portant au moins sur les cinq années précédentes, et pendant un maximum de dix ans, relatif à des infractions pertinentes pour le recrutement à un poste spécifique, dans la Principauté d'Andorre ou dans des pays tiers de résidence au cours de cette période ; iii. Les emplois antérieurs, la formation et toute absence de formation ou d'emploi dans le curriculum vitae de la personne pendant, au minimum, les cinq années précédentes et pendant un maximum de dix ans ; et iv. Toute autre information objective disponible pouvant être nécessaire pour déterminer l'aptitude de la personne intéressée à travailler au poste pour lequel l'entité critique a sollicité des informations.
 - f) Sensibiliser le personnel concerné aux mesures mentionnées aux lettres a) à e).

3. Les mesures adoptées doivent être énumérées et formalisées dans une déclaration d'applicabilité des mesures de sécurité que les entités doivent transmettre à l'autorité nationale compétente dans un délai de six mois à compter de l'identification de l'entité en tant qu'entité essentielle ou importante, conformément à l'article 10, ou à compter de l'entrée en vigueur du Schéma national de sécurité, la date la plus tardive étant retenue, laquelle fera l'objet d'une révision au moins tous les trois ans.
4. Les entités essentielles et importantes doivent adopter des politiques de sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires pour fournir leurs services essentiels et importants, compte tenu des principes de sécurité intégrale, de gestion des risques, de prévention, de réponse et de rétablissement, de lignes de défense, de réévaluation périodique et de séparation des tâches. Les politiques de sécurité des infrastructures critiques, des réseaux et des systèmes d'information doivent contenir, au minimum, les éléments suivants :
 - a) Analyse et gestion des risques.
 - b) Gestion des risques liés aux tiers ou aux fournisseurs.
 - c) Catalogue de mesures de sécurité, organisationnelles, technologiques et physiques.
 - d) Gestion du personnel et professionnalisme.
 - e) Acquisition de produits ou de services de sécurité.
 - f) Détection et gestion des incidents.
 - g) Plans de rétablissement et de garantie de la continuité des opérations.
 - h) Amélioration continue.
 - i) Interconnexion des systèmes.
 - j) Enregistrement de l'activité des utilisateurs.
5. Les autorités nationales compétentes peuvent établir des obligations spécifiques pour garantir la sécurité des infrastructures critiques, des réseaux et des systèmes d'information utilisés par les entités qui fournissent des services essentiels ou importants. De même, elles peuvent édicter des instructions techniques et des guides d'orientation pour détailler le contenu de ces instructions et guides.
6. Pour l'élaboration de dispositions réglementaires, d'instructions et de guides, l'autorité nationale compétente tient compte de toutes les obligations sectorielles et conditions requises en matière de sécurité de l'information auxquelles sont soumis les opérateurs auxquels s'appliquent les dispositions de la présente Loi.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 13. Gestion des risques de cybersécurité

1. Les entités essentielles et importantes, et tout particulièrement celles qui, en plus d'être essentielles, sont critiques, doivent adopter les mesures techniques et organisationnelles adéquates et proportionnées pour établir un processus de gestion des risques qui se présentent, afin d'atteindre un niveau élevé de résilience des infrastructures critiques et de protection des réseaux et des systèmes d'information qu'elles utilisent pour la prestation de leurs services essentiels et importants au regard des risques qui se présentent. Parmi les mesures de gestion du risque doivent figurer celles dont la finalité est de déterminer tout risque d'inci-

dents, de prévenir, de détecter et de gérer les incidents et d'en réduire les répercussions. Ce processus de gestion des risques doit comprendre la sécurité des données stockées, transmises et traitées et, dans le cas des entités essentielles, doit tenir compte de tous les risques pertinents relevés par les autorités nationales compétentes conformément à l'évaluation des risques visée à l'article 6.4.b), ainsi que de toutes les dépendances avec d'autres secteurs et avec des entités critiques ou équivalentes à des entités critiques.

2. L'effort consacré par les entités à la gestion des risques de cybersécurité doit être proportionné aux risques que présentent le réseau et les systèmes d'information qui participent à l'offre de leurs services essentiels et importants, et tenir compte de l'état de la technique. Parmi les critères permettant d'apprécier la proportionnalité des efforts en matière de gestion des risques doivent être pris en considération, au minimum, les suivants :
 - a) La mesure dans laquelle les entités essentielles et importantes utilisent des services, systèmes ou produits TIC critiques et en dépendent ;
 - b) L'importance de services, systèmes ou produits TIC critiques spécifiques pour l'exercice de fonctions critiques ou sensibles, en particulier le traitement de données à caractère personnel ;
 - c) La disponibilité de services, systèmes ou produits TIC de substitution ;
 - d) La résilience de la chaîne d'approvisionnement globale de services, systèmes ou produits TIC face aux perturbations ; et
 - e) Dans le cas des services, systèmes ou produits TIC émergents, le poids qu'ils peuvent avoir à l'avenir pour les activités des entités.
3. Parmi les mesures de gestion des risques qui se présentent doivent figurer, au moins, les éléments suivants :
 - a) La politique de sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires à la prestation de services essentiels ou importants ;
 - b) La politique de gestion des risques ;
 - c) La gestion des incidents (prévention, détection et réponse aux incidents) ;
 - d) La continuité des activités et la gestion de crises ;
 - e) La sécurité de la chaîne d'approvisionnement, y compris les aspects de sécurité relatifs aux relations entre chaque entité et ses fournisseurs ou prestataires de services tels que, par exemple, les fournisseurs de services de stockage et de transformation ou d'analyse de données ou de services de sécurité gérés ;
 - f) La sécurité de l'acquisition, du développement et de la maintenance des infrastructures critiques, des réseaux et des systèmes d'information, y compris la gestion et la divulgation des vulnérabilités ;
 - g) Les politiques et les procédures (essais et audits) permettant d'évaluer l'efficacité des mesures de gestion des risques de cybersécurité ; et
 - h) L'utilisation de la cryptographie et du chiffrement.
4. Les entités doivent tenir compte des vulnérabilités propres à chaque fournisseur et prestataire de services ainsi que de la qualité globale des produits et des pratiques en matière de cybersécurité de leurs fournisseurs et prestataires de services, y compris leurs procédures de développement sécurisé.

5. Lorsqu'une entité constate que ses services ou missions ne sont pas conformes aux conditions requises établies aux paragraphes 1, 2 et 3, elle doit, dans les meilleurs délais, adopter toutes les mesures correctrices nécessaires pour que le service ou la mission en question, satisfasse à ces conditions requises.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 14. Obligation de résoudre les incidents, d'information et de collaboration mutuelle

1. En matière de gestion des incidents de sécurité, de détection de vulnérabilités ou de cybermenaces, les entités essentielles et importantes doivent :
 - a) Gérer et résoudre les incidents de sécurité qui affectent les infrastructures critiques, les réseaux ou les systèmes d'information utilisés pour fournir leurs services essentiels ou importants. S'il s'agit d'infrastructures, de réseaux ou de systèmes externes, il doit être garanti que les fournisseurs externes respectent l'application des mesures nécessaires pour garantir la sécurité.
 - b) Solliciter l'avis ou le soutien spécialisé du CSIRT-AD pour faire face aux incidents, vulnérabilités ou cybermenaces survenus et, en tout état de cause, se conformer aux indications reçues de la part du CSIRT-AD pour résoudre les risques, en atténuer les effets et rétablir les systèmes affectés. Dans ce cas, les indications émises par le CSIRT-AD pour atténuer les effets et rétablir les systèmes affectés sont d'application contraignante.
 - c) Appliquer leur politique de gestion de la sécurité des infrastructures critiques, des réseaux et des systèmes d'information face à la survenance de tout incident affectant la prestation de leurs services essentiels et importants, ainsi que l'ensemble des obligations et recommandations émises par l'autorité nationale compétente ou le CSIRT-AD.
2. Les entités essentielles et importats doivent fournir au CSIRT-AD et à l'autorité nationale compétente concernée toutes les informations qui leur sont demandées pour l'accomplissement des fonctions que leur confie la présente Loi. En particulier, des informations complémentaires peuvent être demandées aux entités essentielles ou importantes pour analyser la nature, les causes et les effets des incidents notifiés, ainsi que pour élaborer des statistiques et réunir les données nécessaires à l'élaboration des rapports annuels prévus à l'article 25.4.e). Lorsque les circonstances le permettent, l'autorité nationale compétente ou le CSIRT-AD fournit aux entités essentielles ou importantes affectées par des incidents les informations découlant de son suivi qui peuvent leur être utiles, en particulier, pour résoudre l'incident.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 15. Obligation de notification

1. Les entités qui fournissent des services essentiels ou importants doivent notifier au CSIRT-AD, qui à son tour le fera auprès de l'autorité nationale compétente dont il relève et en tout état de cause auprès de l'ANC-AD, les incidents qui ont ou peuvent avoir des effets significatifs sur ces services conformément à ce qui est établi par voie réglementaire, ainsi que toute information permettant à l'autorité nationale compétente ou au CSIRT-AD de déterminer les répercussions transfrontières que l'incident peut avoir.

Cette notification doit être effectuée sans retard et en tout état de cause dans un délai de soixante-douze heures à compter de sa détection.

Si, au moment de notifier l'incident ou l'incident possible, elles ne disposent pas encore d'informations relatives à sa répercussion sur des services essentiels ou importants, elles peuvent omettre ces informations, avec l'engagement de les transmettre dans les meilleurs délais, et à l'issue d'un délai de soixante-douze heures à compter de la notification de l'incident, l'entité essentielle ou importante qui n'a pas réuni les informations pertinentes doit adresser au CSIRT-AD un rapport justificatif des actions qu'elle a menées pour obtenir ces informations et des motifs pour lesquels il n'a pas été possible de les obtenir.

Le cas échéant, ces entités doivent notifier, sans retard injustifié, aux destinataires de leurs services susceptibles d'être affectés par l'incident, les mesures ou solutions que ces destinataires peuvent appliquer en réponse à celui-ci.

2. Les entités de services essentiels ou importants doivent notifier à l'autorité nationale compétente, par l'intermédiaire du CSIRT-AD et sans retard, toute cybermenace significative pour les services essentiels ou importants qui, à leur avis, peut aboutir à un incident significatif conformément à ce qui est établi par voie réglementaire. Le cas échéant, ces entités doivent notifier, sans retard injustifié, aux destinataires de leurs services susceptibles d'être affectés par une cybermenace significative, les mesures ou solutions que ces destinataires peuvent appliquer en réponse à la menace. Le cas échéant, les entités notifient aux destinataires la menace elle-même.
3. Une menace significative est celle qui peut donner lieu à un incident significatif, et un incident est considéré comme significatif si :
 - a) L'incident a causé ou peut causer des perturbations opérationnelles ou des préjudices économiques substantiels pour l'entité concernée ; ou
 - b) L'incident a affecté ou peut affecter d'autres personnes physiques ou morales en causant des préjudices matériels ou moraux considérables en ce qui concerne : i. Le nombre d'utilisateurs affectés par la perturbation du service essentiel et sa part de marché. ii. La durée de l'incident. iii. L'absence d'alternatives pour maintenir un niveau suffisant de fourniture du service. iv. L'étendue ou les zones géographiques affectées ou susceptibles d'être affectées par l'incident. v. Le degré de perturbation du fonctionnement du service. vi. La portée de l'impact sur des activités économiques et sociales cruciales. vii. L'importance des systèmes affectés ou des informations affectées par l'incident pour la fourniture du service essentiel. viii. La dépendance d'autres secteurs stratégiques à l'égard du service et la répercussion, en termes de degré et de durée, de l'incident sur les activités sociales et économiques ou sur la sécurité publique. ix. L'atteinte à la réputation. Des facteurs spécifiques au secteur peuvent être ajoutés par voie réglementaire pour déterminer si un incident peut avoir des effets perturbateurs significatifs.
4. En ce qui concerne les notifications visées aux paragraphes 1 et 2, les entités concernées doivent présenter au CSIRT-AD :
 - a) Une notification initiale sans retard injustifié et en tout état de cause dans un délai de vingt-quatre heures à compter de la prise de connaissance de l'incident, dans laquelle il est indiqué, le cas échéant, s'il y a lieu de supposer que l'incident résulte d'une action illícite ou malveillante ; b) Toutes les notifications intermédiaires qui s'avèrent nécessaires ou

que le CSIRT-AD demande afin de mettre à jour ou de compléter les informations figurant dans la notification initiale et d'informer sur l'évolution de l'incident tant que celui-ci n'est pas résolu ; et

- c) Un rapport final, au plus tard un mois après la présentation de la notification initiale prévue à la lettre a), dans laquelle figurent au moins les éléments suivants : i. une description détaillée de l'incident, de sa gravité et de son impact ; ii. le type de menace ou la cause principale qui a probablement déclenché l'incident ; et iii. les mesures d'atténuation appliquées et en cours.
5. Dans des cas dûment justifiés, tels que des cas de force majeure, l'entité peut ne pas respecter les délais établis aux paragraphes 1 et 2.
6. Les notifications effectuées en vertu du présent article doivent inclure les informations permettant de déterminer tout effet transfrontière de l'incident.
7. Le CSIRT-AD fournit, dans un délai de vingt-quatre heures après la réception de la notification initiale visée au paragraphe 4.a), une réponse à l'entité qui a effectué la notification, comprenant notamment ses commentaires initiaux sur l'incident et, à la demande de l'entité, des orientations sur l'application d'éventuelles mesures d'atténuation. Le CSIRT-AD apporte un soutien technique supplémentaire lorsque l'entité concernée le demande. Lorsqu'il est soupçonné que l'incident est de nature délictueuse, le CSIRT-AD fournit également des orientations aux fins de signaler l'incident aux autorités compétentes. L'obligation de notification d'incidents prévue au présent article ne dispense pas de l'accomplissement du devoir général qu'a l'entité qui effectue la notification de dénoncer auprès des autorités compétentes les faits susceptibles de revêtir un caractère délictueux.
8. Lorsque la connaissance du public est nécessaire pour prévenir un incident ou faire face à un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public, l'ANC-AD, avec le soutien du CSIRT-AD, peut informer le public de l'incident, après consultation de l'entité concernée, ou exiger de l'entité qu'elle le fasse si celle-ci n'a pas agi préalablement en ce sens.
9. Les notifications des entités essentielles doivent porter sur les incidents qui affectent les infrastructures critiques, les réseaux et les systèmes d'information utilisés pour la fourniture des services essentiels, qu'il s'agisse indifféremment d'infrastructures critiques, de réseaux et de systèmes propres ou de fournisseurs externes.
10. Les entités essentielles ou importantes doivent effectuer les notifications qui leur incombent en vertu du présent chapitre par l'intermédiaire du Délégué à la sécurité de l'information (DSI) qu'elles ont désigné conformément aux dispositions de l'article 18.
11. La notification d'un incident conformément aux dispositions de la présente Loi n'exclut ni ne remplace l'obligation de notification que les entités doivent effectuer auprès d'autres organismes conformément à leur réglementation spécifique.
12. Lorsque la notification d'incidents ou leur gestion, leur analyse ou leur résolution requiert la communication de données à caractère personnel, leur traitement doit être limité aux données strictement adéquates, pertinentes et limitées au regard de la finalité poursuivie dans chaque cas. Les communications de données à caractère personnel à ces fins sont réputées autorisées dans les cas suivants :

- a) Entre les entités essentielles ou importantes et l'ANC-AD, le CSIRT-AD ou les autorités nationales compétentes.
- b) Entre le CSIRT-AD et l'ANC-AD.
- c) Entre le CSIRT-AD et d'autres CSIRT désignés au niveau international.
- d) Entre l'ANC-AD et d'autres autorités compétentes internationales.
- e) Entre les autorités nationales compétentes et l'ANC-AD.
- f) Entre les autorités nationales compétentes et le CSIRT-AD.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 16. Notification volontaire

1. Sans préjudice des dispositions de l'article 2, les entités exclues du champ d'application de la présente Loi peuvent présenter volontairement des notifications de cybermenaces, d'incidents évités et d'incidents significatifs. Lorsqu'elles transmettent les notifications au CSIRT-AD, ces entités agissent conformément à la procédure établie à l'article 15.
 2. De même, les entités essentielles ou importantes peuvent notifier les incidents ou les cybermenaces pour lesquels aucune obligation de notification n'est établie.
 3. Ces notifications obligent l'entité qui les a effectuées à résoudre l'incident conformément aux dispositions de la présente Loi. Toutefois, ce type d'entité notifiante n'est pas soumis à d'autres obligations supplémentaires auxquelles il n'aurait pas été tenu s'il n'avait pas présenté cette notification.
 4. Les notifications obligatoires ont un caractère prioritaire sur les notifications volontaires aux fins de leur traitement par le CSIRT-AD.
- ### Chapitre II. Autres obligations des entités essentielles et importantes

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 17. Gouvernance

1. Les organes de direction des entités essentielles et importantes doivent approuver les mesures de gestion des risques en matière de cybersécurité adoptées par ces entités conformément aux dispositions de l'article 13, superviser leur mise en œuvre et répondre du non-respect, par les entités, des obligations prévues audit article.
2. Les membres de l'organe de direction doivent suivre périodiquement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes leur permettant de comprendre et d'évaluer les risques en matière de cybersécurité et les pratiques de gestion, ainsi que leur impact sur les opérations de l'entité.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 18. Délégué à la Sécurité de l'Information

1. Les entités essentielles et les entités importantes, par l'intermédiaire de leurs organes de direction, doivent désigner une personne physique, une unité ou un organe collégial, afin qu'il agisse en tant que Délégué à la Sécurité de l'Information (DSI) et soit le point de contact et

de coordination technique entre l'entité qui l'a désigné et l'autorité nationale compétente et le CSIRT-AD.

2. Lorsque le DSI est une unité ou un organe collégial, une personne physique le représentant est désignée.
3. En tout état de cause, les entités essentielles ou importantes doivent également désigner un suppléant du DSI afin qu'il assume ses fonctions en cas d'absence, de vacance ou de maladie.
4. Les coordonnées du DSI en fonctions doivent être notifiées à l'autorité compétente dans un délai maximal d'un mois à compter de la date de la désignation correspondante. La même procédure est suivie en cas de modification des coordonnées, par exemple en raison de cessations de fonctions ou de nominations, celles-ci devant être notifiées à l'autorité nationale compétente, qui à son tour les communique immédiatement au CSIRT-AD, dans un délai maximal d'un mois à compter de la date de la modification.
5. Le DSI agit en tant que point de contact pour notifier les incidents conformément à l'article 15, ainsi que pour gérer ce qui est approprié au sein de l'entité qui l'a nommé, conformément aux articles 13 et 14.
6. En outre, à titre indicatif et non limitatif, le DSI exerce, sous la responsabilité de l'entité qui l'a nommé, les fonctions suivantes :
 - a) Élaborer et proposer, conformément aux dispositions de l'article 12, des politiques de sécurité, comprenant une proposition de mesures techniques et organisationnelles, adéquates et proportionnées, pour prévenir et gérer les risques éventuels relatifs à la sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires à la fourniture des services essentiels ou importants, afin de réduire au minimum les effets des cyberincidents qui affectent lesdits services.
 - b) Élaborer le document de déclaration d'applicabilité des mesures de sécurité en relation avec le Schéma National de Sécurité de la Principauté d'Andorre.
 - c) Superviser l'application des politiques de sécurité, des protocoles et des procédures au sein de l'entité, superviser leur efficacité et établir des périodes de contrôle.
 - d) Promouvoir la formation et l'application de bonnes pratiques en matière de sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires à la fourniture des services essentiels ou importants qu'offre l'entité qui les a désignés comme DSI.
 - e) Transmettre au CSIRT-AD, qui à son tour informe l'autorité nationale compétente, sans retard injustifié, les notifications d'incidents, de vulnérabilités ou de cybermenaces ayant des effets perturbateurs sur la prestation des services essentiels ou importants.
 - f) Recevoir, interpréter, superviser et transmettre l'application des instructions et des guides émanant de l'autorité nationale compétente ou du CSIRT-AD.
 - g) Recueillir, préparer et fournir des informations ou de la documentation à l'autorité nationale compétente ou au CSIRT-AD lorsque ceux-ci le demandent ou de sa propre initiative.
 - h) Échanger des informations pertinentes en matière de cybersécurité directement avec les DSI d'autres entités essentielles et importantes autorisées par l'entité qui l'a nommé, ou au moyen des canaux de communication que l'ANC-AD peut établir à cet effet, et en particulier des informations relatives aux cybermenaces, aux vulnérabilités, aux indicateurs de

compromission, aux déclarations d'applicabilité, aux tactiques, techniques et procédures, aux alertes de cybersécurité et aux outils de configuration, pour autant que cet échange d'informations : i. ait pour objectif de prévenir les cybermenaces éventuelles, de les décourager, de les détecter, et de répondre aux incidents ou de les atténuer ; ii. renforce le niveau de cybersécurité, en particulier en sensibilisant aux cybermenaces, limite ou empêche la capacité de telles menaces à se propager, ou soutienne une série de capacités de défense, de correction et de divulgation des vulnérabilités, de techniques de détection des menaces, de stratégies d'atténuation ou d'étapes de réponse et de rétablissement. Cet échange est mis en œuvre au moyen de mécanismes d'échange d'informations qui respectent la nature éventuellement sensible des informations partagées, et conformément à ce qui peut être établi par voie réglementaire.

7. Le DSI peut faire partie de l'effectif salarié de l'entité qui le nomme ou exercer ses fonctions dans le cadre d'un contrat de services.
8. Les entités essentielles et importantes doivent garantir, à titre indicatif et non limitatif, que le DSI :
 - a) Soit une personne ou un groupe de personnes disposant de connaissances spécialisées et d'expérience en matière de cybersécurité, tant du point de vue organisationnel que du point de vue technique et juridique, en vertu des fonctions attribuées au paragraphe 6.
 - b) Se voie garantir les ressources nécessaires à l'exercice de ses fonctions.
 - c) Se voie attribuer une position au sein de l'organisation de l'entité qui facilite l'exercice de ses fonctions afin de pouvoir participer de manière appropriée, et en temps utile, à toutes les questions relatives à la sécurité, ainsi que le maintien d'une communication réelle et effective avec la haute direction.
 - d) Soit son indépendance assurée vis-à-vis des responsables des infrastructures critiques, des réseaux et des systèmes d'information de son domaine de travail.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 19. Représentant dans la Principauté d'Andorre

1. Si une entité qui fournit des services essentiels ou importants dans la Principauté d'Andorre n'y est pas établie, elle désigne un représentant dans la Principauté d'Andorre qui soit soumis à la juridiction du pays. En l'absence de ce représentant, l'ANC-AD peut identifier l'entité essentielle ou importante, l'informer de ses obligations prévues par la présente Loi et engager des actions en justice contre elle pour le non-respect de celles-ci.
2. La désignation d'un représentant par une entité visée au paragraphe 1 s'entend sans préjudice des actions en justice qui peuvent être engagées contre l'entité elle-même.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 20. Utilisation de schémas de certification de cybersécurité

1. Aux fins de démontrer la conformité à certaines conditions requises établies par la présente Loi, les autorités nationales compétentes peuvent exiger des entités essentielles et importantes, ou de catégories d'entités essentielles ou importantes, relevant de leur domaine de compétence, qu'elles certifient certains produits, services et processus TIC en vertu d'un

schéma de certification de cybersécurité spécifique adopté par voie réglementaire. Les produits, services ou processus faisant l'objet de la certification peuvent être développés par l'entité essentielle ou importante ou acquis auprès de tiers.

2. De même, dès lors qu'un schéma de certification d'un domaine de la cybersécurité a été établi par voie réglementaire, les autorités nationales compétentes peuvent délivrer un certificat relatif audit domaine aux entités essentielles ou importantes qui justifient du respect des obligations de sécurité des infrastructures critiques, des réseaux et des systèmes d'information correspondants.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 21. Protection de l'auteur de la notification

1. La notification volontaire ne peut donner lieu à l'imposition à l'entité notifiante d'obligations supplémentaires auxquelles elle ne serait pas soumise si elle n'avait pas présenté cette notification.
2. Le DSI qui effectue la notification, qu'il ait une relation de travail ou commerciale avec l'entité qui l'a nommé, ou la personne qui effectue la notification dans le cas d'entités non assujetties, ne peut en aucun cas subir de conséquences négatives à son poste de travail ou dans sa relation avec l'entité du fait qu'il procède à la notification d'un incident conformément aux dispositions de la présente Loi, sauf dans les cas où sa mauvaise foi est établie.
3. Sont nulles et dépourvues d'effet juridique toutes les décisions de l'employeur prises au préjudice ou au détriment des droits du travail des travailleurs ayant agi conformément aux dispositions de l'article 15 ou de l'article 16.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Chapitre troisième. Obligations de supervision

Article 22. Supervision du respect des obligations de sécurité et des notifications d'incidents

1. Chaque autorité nationale compétente est chargée de superviser le respect de la présente Loi, et notamment des obligations décrites aux articles 13 et 15, applicables aux entités essentielles et importantes relevant de son domaine d'action compétent.
2. Chaque entité essentielle ou importante doit collaborer avec son autorité nationale compétente dans le cadre de ladite supervision, faciliter les opérations de contrôle fiscal, fournir toutes les informations qui lui sont demandées à cet effet et appliquer les instructions édictées.
3. Chaque autorité nationale compétente peut mener les opérations d'inspection nécessaires à l'exercice de ses fonctions de contrôle dans son domaine de compétence lorsqu'elles ont pour objet :
 - a) De contrôler le respect des normes et instructions techniques qui, le cas échéant, sont applicables aux entités soumises à sa supervision.

- b) De vérifier l'exercice des fonctions du DSI désigné au sein des entités de services essentiels et importants.
 - c) D'effectuer les inspections, vérifications, tests et examens nécessaires pour vérifier le respect des mesures de sécurité prévues par la présente Loi et, en particulier, l'applicabilité de la politique de sécurité des entités et l'application des mesures de sécurité pertinentes.
4. Chaque fois qu'une autorité nationale compétente le demande, le CSIRT-AD doit collaborer à l'exercice des fonctions visées au paragraphe précédent. En particulier, le CSIRT-AD doit fournir des conseils techniques sur l'adéquation des mesures de sécurité adoptées par les entités pour fournir leurs services essentiels ou importants.

Redacció vigent des del 23/06/2024 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 23. Supervision et exécution dans le cas des entités essentielles

1. Chaque autorité nationale compétente doit veiller à ce que les entités essentielles relevant de son domaine de compétence respectent les obligations établies par la présente Loi de manière effective, proportionnée et dissuasive.
2. Les compétences des autorités nationales compétentes, en coopération avec le CSIRT-AD le cas échéant, en matière de supervision, se fondent sur :
 - a) Des inspections sur place et une supervision à distance, y compris des contrôles aléatoires ;
 - b) Des audits périodiques ;
 - c) Des audits de sécurité spécifiques fondés sur des évaluations des risques ou sur des informations disponibles relatives aux risques ;
 - d) Des analyses de sécurité au moyen de critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents ;
 - e) Des demandes de toutes les informations nécessaires pour évaluer les mesures de cybersécurité adoptées par l'entité, en particulier les politiques de cybersécurité documentées, ainsi que le respect de la procédure de notification prévue par la présente Loi, si nécessaire ;
 - f) Des demandes d'accès à des données, documents ou toute information nécessaire à l'exercice de ses fonctions de supervision ; et
 - g) Des demandes de tout type de preuves nécessaires pour justifier l'application des politiques de cybersécurité. En ce qui concerne les lettres e),
- f) et g), l'autorité nationale compétente doit à tout moment indiquer la finalité de la demande et préciser les informations requises.
3. Les compétences des autorités nationales compétentes, en coopération avec le CSIRT-AD le cas échéant, en matière d'exécution, se fondent sur :
 - a) Adresser un avertissement aux entités pour le non-respect des obligations établies par la présente Loi.
 - b) Émettre des instructions contraignantes afin que les entités corrigent les défaillances détectées ou les manquements aux obligations établies par la présente Loi.

- c) Exiger des entités qu'elles mettent fin aux comportements qui enfreignent les obligations établies par la présente Loi et qu'elles s'abstiennent de les réitérer.
 - d) Exiger des entités qu'elles mettent leurs mesures de gestion des risques ou leurs obligations de notification en conformité avec les dispositions du chapitre premier du présent Titre.
 - e) Ordonner aux entités d'informer les personnes physiques ou morales auxquelles elles fournissent des services qui sont susceptibles d'être affectées par une cybermenace importante, ainsi que des mesures correctives ou de protection correspondantes que lesdites personnes peuvent adopter en réponse à la menace.
 - f) Ordonner aux entités la mise en œuvre, dans un délai raisonnable, des recommandations formulées à la suite d'un audit de sécurité.
 - g) Désigner un responsable de la supervision pour exercer des fonctions clairement définies et pour superviser, pendant une période déterminée, le respect de leurs obligations prévues au Titre III.
 - h) Ordonner aux entités de rendre publics, d'une manière déterminée, les manquements aux obligations établies par la présente Loi.
 - i) Émettre des communiqués publics identifiant les personnes physiques et morales responsables de manquements aux obligations établies par la présente Loi et la nature desdits manquements.
 - j) Imposer, dans le cas de l'ANC-AD, ou demander l'imposition par l'ANC-AD, dans le cas de l'AFa, d'une amende administrative conformément aux dispositions du Titre IV, à titre complémentaire ou en remplacement des mesures visées aux lettres
- a) à
- i) du présent paragraphe, en fonction des circonstances de chaque cas particulier.
4. Lorsque les mesures d'exécution exigées par l'autorité nationale compétente ne sont pas adoptées dans le délai établi, l'autorité nationale compétente est habilitée à :
- a) Suspendre la certification de conformité ;
 - b) Imposer une interdiction temporaire à toute personne physique exerçant des responsabilités de direction ou de représentation légale de l'entité essentielle, ainsi qu'à toute autre personne physique responsable du manquement, d'exercer des fonctions de direction dans cette entité. Ces suspensions ou interdictions demeurent jusqu'à ce que l'entité concernée adopte les mesures nécessaires pour remédier aux défaillances ou satisfasse aux conditions requises par l'autorité nationale compétente qui a appliqué la suspension ou l'interdiction en question.
5. Les mesures indiquées au paragraphe précédent s'appliquent sans préjudice de garantir le droit de la défense de la personne concernée, au moins pour les aspects suivants :
- a) La gravité du manquement et l'importance des obligations enfreintes, et en particulier celles qualifiées de graves et de très graves conformément à l'article 34 ;
 - b) La durée du manquement, notamment s'il y a eu des manquements réitérés ;
 - c) Les préjudices ou les pertes réels occasionnés, ou les préjudices ou les pertes qui auraient pu être occasionnés, dans la mesure où ils peuvent être déterminés, compte tenu notam-

- ment des pertes financières ou économiques réelles ou potentielles, des effets sur d'autres services et du nombre d'utilisateurs affectés ou potentiellement affectés ;
- d) Le caractère intentionnel ou la négligence de l'infraction ;
 - e) Les mesures adoptées par l'entité pour prévenir ou atténuer les préjudices ou les pertes ;
 - f) L'adhésion à des codes de conduite ou à des mécanismes de certification approuvés ; et
 - g) Le degré de coopération des personnes physiques ou morales responsables avec les autorités nationales compétentes.
6. L'autorité nationale compétente doit émettre les décisions d'exécution de manière détaillée et motivée, en les notifiant préalablement à leur émission définitive aux entités concernées, en leur accordant un délai de six mois pour formuler des observations.

Redacció vigent des del 23/06/2024 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 24

Supervision et exécution dans le cas d'entités importantes

1. Si l'autorité nationale compétente dispose de preuves ou d'indices de manquement aux obligations établies dans la présente Loi, de la part d'une entité de services importants, ladite autorité peut imposer a posteriori les mesures de supervision correspondantes.
2. À cet égard, les compétences de l'autorité nationale compétente, en coopération avec le CSIRT-AD, le cas échéant, en matière de supervision, se fondent sur :
 - a) Des inspections sur place et une supervision a posteriori ;
 - b) Des audits de sécurité spécifiques fondés sur des évaluations des risques ou sur les informations disponibles concernant les risques ;
 - c) Des analyses de sécurité fondées sur des critères d'évaluation des risques objectifs, équitables et transparents ;
 - d) Des demandes de toute information nécessaire pour évaluer a posteriori les mesures de cybersécurité, en particulier les politiques de cybersécurité documentées, ainsi que le respect des obligations de notifier les incidents à l'autorité nationale compétente ; et
 - e) Demander l'accès à des données ou à toute information nécessaire au bon exercice des fonctions de supervision. En ce qui concerne les lettresd) et e), l'autorité nationale compétente doit, à tout moment, indiquer la finalité de la demande et préciser les informations requises.
3. Les compétences de l'autorité nationale compétente, en coopération avec le CSIRT-AD, le cas échéant, en matière d'exécution, se fondent sur :
 - a) Adresser des avertissements aux entités pour manquement aux obligations établies dans la présente Loi.
 - b) Émettre des instructions contraignantes afin que les entités remédient aux défaillances détectées ou aux violations des obligations établies dans la présente Loi.
 - c) Exiger des entités qu'elles mettent fin aux comportements qui contreviennent aux obligations établies dans la présente Loi et qu'elles s'abstiennent de les réitérer ;
 - d) Exiger des entités qu'elles mettent leurs mesures de gestion des risques ou leurs obligations de notification en conformité avec les dispositions du Titre III.

- e) Ordonner aux entités d'informer les personnes physiques ou morales auxquelles elles fournissent des services qui sont susceptibles d'être affectées par une cybermenace importante ainsi que des mesures correctives ou de protection correspondantes que les personnes affectées peuvent adopter en réponse à la menace.
 - f) Ordonner aux entités la mise en œuvre, dans un délai raisonnable, des recommandations formulées à la suite d'un audit de sécurité.
 - g) Désigner un responsable de la supervision chargé d'exercer des fonctions clairement définies et de superviser, pendant une période déterminée, le respect des obligations prévues au Titre III.
 - h) Ordonner aux entités de rendre publics, d'une manière déterminée, les manquements aux obligations établies dans la présente Loi.
 - i) Émettre des communiqués publics dans lesquels sont identifiées les personnes physiques et morales responsables de manquements aux obligations établies dans la présente Loi ainsi que la nature desdits manquements.
 - j) Imposer ou demander l'imposition d'une amende administrative conformément aux dispositions du Titre IV, à titre complémentaire ou en remplacement des mesures visées aux lettres
 - a) à
 - i) du présent paragraphe, en fonction des circonstances de chaque cas particulier.
4. Les dispositions des paragraphes 4 à 6 de l'article 23 sont également applicables aux entités importantes.

Redacció vigent des del 23/06/2024 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Chapitre quatrième. Autres obligations des autorités nationales compétentes et du CSIRT-AD

Article 25. Obligations des autorités nationales compétentes

1. Les autorités nationales compétentes au titre de la présente Loi doivent coopérer et échanger des informations avec les responsables de la rédaction des règlements ou autres normes ou actes juridiques sectoriels, en particulier en ce qui concerne la gestion des risques de cybersécurité et des incidents affectant les entités essentielles ou importantes, ainsi qu'en ce qui concerne les mesures de cybersécurité adoptées par ces entités.
2. Les autorités nationales compétentes doivent établir les canaux favorisant la communication avec les entités qui fournissent des services essentiels et importants, susceptibles d'être développés par voie réglementaire.
3. Les autorités nationales compétentes doivent se coordonner avec le CSIRT-AD au moyen des protocoles d'action qui, le cas échéant, peuvent être développés par voie réglementaire.
4. L'ANC-AD, en collaboration avec l'AFA et avec le CSIRT-AD, doit :
 - a) Établir une liste des entités identifiées au titre des points
 - b) à

- f) de l'article 2.2 dans le délai de six mois à compter de la date d'entrée en vigueur de la présente Loi, liste qu'elle révisé périodiquement, au moins tous les deux ans, et qu'elle met à jour le cas échéant.
- b) Créer et tenir un registre des entités essentielles et importantes.
- c) Notifier, sans retard injustifié, aux agences de cybersécurité existant dans d'autres pays tout incident ou toute cybermenace ayant un impact transfrontière ou susceptible de leur porter préjudice ou de les affecter de toute autre manière et dont le niveau est considéré comme significatif conformément aux dispositions de l'article 15.3. Ce faisant, l'ANC-AD préserve, conformément à la législation en vigueur à tout moment, la sécurité et les intérêts commerciaux de l'entité ayant notifié l'incident, ainsi que la confidentialité des informations fournies.
- d) Coopérer, dans le champ d'application de la présente Loi, avec l'Agence andorrane de protection des données (APDA) et les autorités publiques compétentes en matière de sécurité publique, de sécurité civile et de sécurité nationale, y compris par la communication sans délai de tout incident susceptible de relever du champ de supervision de chaque autorité, et les tenir informées de l'évolution de ces incidents.
- e) Émettre des rapports annuels à l'intention du Gouvernement d'Andorre sur les incidents, les quasi-incidents et les cybermenaces notifiés par les entités essentielles et importantes, l'état de la mise en œuvre de la Stratégie nationale de cybersécurité et la situation de la cybersécurité dans la Principauté d'Andorre. Ces rapports de situation comprennent, à titre informatif et non limitatif, entre autres : i. L'évolution des capacités de cybersécurité dans la Principauté d'Andorre. ii. Les ressources techniques, financières et humaines dont disposent les autorités nationales compétentes et le CSIRT-AD. iii. Les politiques de cybersécurité et l'applicabilité des mesures de supervision et d'exécution en fonction des résultats issus du rapport précédent. iv. Un indice de cybersécurité fournissant une évaluation du niveau de maturité des capacités de cybersécurité et établi selon des méthodologies reconnues au niveau international.
- f) Émettre et publier des rapports annuels sur la situation de la cybersécurité dans la Principauté d'Andorre.
- g) Comparaitre, par l'intermédiaire de sa personne de tutelle, devant la commission législative du Conseil général chargée des questions en matière de cybersécurité, afin de présenter les rapports annuels prévus aux lettres
- e) et f), relatifs aux incidents, quasi-incidents et cybermenaces notifiés par les entités essentielles et importantes, à l'état de la mise en œuvre de la Stratégie nationale de cybersécurité et à la situation de la cybersécurité dans la Principauté d'Andorre.
- h) Veiller, afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, à ce que les registres de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine de premier niveau : i. Collectent et conservent des données d'enregistrement de noms de domaine dans une base de données qui : • Contient les informations pertinentes permettant d'identifier et de contacter les titulaires des noms de domaine et les points de contact qui administrent les noms de domaine dans les domaines de premier niveau. • Dispose de politiques et de procédures, mises à la disposition du public, afin de garantir qu'elle comprend des informations exactes et complètes. ii. Publient, sans retard injustifié après l'enregistrement d'un nom de domaine, les données

d'enregistrement de domaine qui ne revêtent pas un caractère personnel. iii. Accordent l'accès à des données spécifiques d'enregistrement de noms de domaine, sur demande licite et dûment justifiée, aux demandeurs d'accès légitimes, conformément à la réglementation de la Principauté d'Andorre en matière de protection des données en vigueur à tout moment.

5. Afin de promouvoir une application convergente avec celle des États voisins, les autorités nationales compétentes publient un cadre normatif par lequel elles encouragent, sans imposer ni favoriser l'utilisation d'un type particulier de technologie, l'utilisation de normes et de spécifications acceptées au niveau international qui sont pertinentes en matière de sécurité des infrastructures critiques, des réseaux et des systèmes d'information de chaque secteur relevant de leur domaine de compétence.
6. Outre les obligations précédentes, les autorités nationales compétentes peuvent établir des obligations spécifiques pour garantir la sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires à la fourniture de services essentiels ou importants ainsi qu'en ce qui concerne la notification des incidents, et édicter des instructions techniques et des guides d'orientation pour préciser le contenu de ces obligations.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 26. Obligations du

CSIRT-AD

1. Le CSIRT-AD a pour principales obligations de :

- a) Garantir la disponibilité de ses services de communication, en établissant divers canaux de communication pour être contacté et pour le contacter directement et à tout moment, en évitant les erreurs ponctuelles simples.
- b) Préciser les canaux et les voies de communication et les faire connaître à ses groupes d'intérêt.
- c) Garantir que ses installations et ses systèmes d'information nécessaires à la réalisation de l'objectif de la présente Loi sont situés dans des lieux sûrs.
- d) Disposer d'un système adéquat pour gérer et acheminer les demandes.
- e) Disposer d'un personnel suffisant pour garantir à tout moment la disponibilité des services qu'il fournit en relation avec la présente Loi.
- f) Maintenir l'accès continu aux infrastructures de communication, en renforçant les systèmes redondants et les espaces de travail de secours afin de sauvegarder la continuité de son activité en relation avec ce qui est prévu dans la présente Loi.
- g) Fournir aux entités essentielles ou importantes susceptibles d'être affectées par des incidents les informations qui peuvent leur être utiles pour prévenir et, le cas échéant, résoudre lesdits incidents.
- h) Fournir aux entités essentielles ou importantes ayant effectué une notification les informations pertinentes relatives au suivi de la notification d'un incident, en particulier celles qui peuvent faciliter la gestion efficace de l'incident.
- i) Garantir la capacité de participer, le cas échéant, à des réseaux de coopération internationale.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 27. Coopération nationale

1. L'ANC-AD, l'AFA et le CSIRT-AD coopèrent entre eux pour veiller au respect des obligations établies dans la présente Loi.
2. L'ANC-AD et le CSIRT-AD coopèrent entre eux pour garantir la réception des notifications d'incidents, d'incidents évités, de vulnérabilités ou de cybermenaces importants, dans le cadre de la présente Loi et avec le soutien des autorités publiques de la Principauté d'Andorre.
3. L'ANC-AD, l'AFA et le CSIRT-AD doivent consulter, lorsqu'il y a lieu, les organes compétents en matière de sécurité nationale, de sécurité publique, de sécurité civile et de protection des données à caractère personnel, et doivent collaborer avec eux dans l'exercice de leurs fonctions respectives établies par la présente Loi.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 28. Coopération transfrontalière

1. Lorsqu'il y a lieu, les autorités nationales compétentes et le CSIRT-AD doivent coopérer avec les autorités compétentes d'autres pays lorsque celles-ci requièrent la supervision visée aux articles 23 et 24 et l'adoption de mesures par des entités essentielles ou importantes pour leurs pays et qui ont un lien avec la Principauté d'Andorre. Cette coopération implique, au minimum, ce qui suit :
 - a) que les autorités nationales compétentes qui appliquent des mesures de supervision ou d'exécution dans la Principauté d'Andorre informent et consultent les autorités compétentes des autres pays concernés au sujet des mesures de supervision et d'exécution adoptées et de leur suivi, conformément aux dispositions des articles 23 et 24 ;
 - b) qu'une autorité compétente étrangère puisse demander à une autorité nationale compétente d'adopter les mesures de supervision ou d'exécution visées aux articles 23 et 24 ;
 - c) qu'une autorité nationale compétente, lorsqu'elle reçoit une demande justifiée d'une autorité compétente étrangère, prête assistance à cette dernière afin que les mesures de supervision ou d'exécution visées aux articles 23 et 24 puissent être appliquées de manière effective, efficiente et cohérente. Cette assistance peut couvrir des demandes d'informations et des mesures de supervision, y compris les demandes de réalisation d'inspections sur place, de supervision à distance ou d'audits de sécurité ciblés. Les autorités nationales compétentes ou le CSIRT-AD peuvent refuser de coopérer avec des autorités compétentes d'autres pays lorsque, après dialogue avec les autres autorités nationales compétentes et l'ANC-AD, l'ANC-AD détermine soit que l'autorité compétente étrangère n'est pas compétente pour demander l'assistance requise, soit que cette assistance n'est adaptée ni aux missions du CSIRT-AD ni aux missions de supervision de l'autorité nationale compétente concernée exercées conformément aux articles 23 et 24.
2. Réciproquement, lorsqu'il y a lieu, les autorités nationales compétentes ou le CSIRT-AD peuvent demander la coopération d'autorités compétentes ou de CSIRT d'autres pays lorsqu'ils requièrent la supervision visée aux articles 23 et 24 ou l'adoption de mesures par des entités essentielles ou importantes pour la Principauté d'Andorre et qui sont établies ou représentées dans ces autres pays, indépendamment du fait que ledit établissement soit ou

non l'établissement principal de l'entité et, dans le cas des entités qui fournissent des services essentiels pour la Principauté d'Andorre, même lorsque celle-ci est représentée dans le pays.

3. Le cas échéant et d'un commun accord, les autorités compétentes de la Principauté d'Andorre et celles d'autres pays peuvent entreprendre conjointement les mesures de supervision visées aux articles 23 et 24.
4. Si le CSIRT-AD ou l'ANC-AD ou l'AFA reçoivent des notifications de la part de pays tiers concernant des incidents qui affectent directement ou indirectement des entités essentielles ou importantes de la Principauté d'Andorre, ils doivent se le notifier immédiatement entre ces entités et le notifier aux entités affectées, afin qu'ils adoptent conjointement les mesures pertinentes dans l'exercice de leurs fonctions respectives.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 29. Confidentialité des informations sensibles

1. L'ANC-AD, l'AFA et le CSIRT-AD doivent préserver la sécurité et les intérêts commerciaux des entités essentielles ou importantes, ainsi que la confidentialité des informations qu'ils obtiennent de celles-ci dans l'exercice des fonctions que leur confie la présente Loi.
 2. Lorsque l'échange d'informations est nécessaire et qu'il s'agit d'informations sensibles, la communication doit être limitée conformément à la correcte application des principes de minimisation de l'information et de proportionnalité au regard de la finalité de cet échange.
- ### IV. Régime de sanctions

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 30. Pouvoir de sanction

1. Tout acte contraire aux dispositions de la présente Loi ou aux dispositions réglementaires prises pour son application peut donner lieu à l'ouverture d'un dossier de sanction et à l'imposition de sanctions après l'instruction préalable du dossier correspondant.
2. Le pouvoir d'ouvrir et de statuer sur les dossiers de sanction en raison des dispositions de la présente Loi appartient à l'autorité qui est, à chaque moment, à la tête de l'ANC-AD, y compris en ce qui concerne les entités qui sont sous la supervision de l'AFA, à la demande de cette dernière. L'instruction des dossiers incombe aux techniciens désignés par l'ANC-AD.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 31. Responsables des infractions

Sont responsables des infractions à l'égard de ce que régit la présente Loi les entités essentielles et importantes soumises au respect des préceptes établis dans celle-ci.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 32. Dossier de sanction

1. La constatation d'une infraction par l'autorité nationale compétente concernée entraîne l'ouverture du dossier de sanction correspondant par l'autorité qui dispose du pouvoir de sanction, conformément aux dispositions de la réglementation en vigueur à tout moment en ma-

tière de procédures administratives de sanction. Toutefois, le délai maximal de durée de la procédure est d'un an, tandis que le délai d'observations ne peut avoir une durée inférieure aux six mois indiqués à l'article 23.6.

2. Les procès-verbaux de l'ANC-AD bénéficient de la présomption d'exactitude, sauf preuve contraire.
3. Les décisions rendues par l'autorité qui dispose du pouvoir de sanction peuvent faire l'objet d'un recours, conformément aux dispositions de la réglementation en vigueur à tout moment en matière de recours administratifs.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 33. Infractions

Constituent des infractions à ce que régit la présente Loi les actions ou omissions contraires aux dispositions de ses préceptes.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 34. Classification des infractions

1. Les infractions aux préceptes contenus dans la présente Loi sont classées en très graves, graves et légères.
2. Constituent des infractions très graves :
 - a) Le défaut de transmission des informations relatives à l'obligation d'identification en tant qu'entité essentielle ou importante, conformément aux dispositions de l'article 10, lorsque celle-ci dispose d'un établissement dans la Principauté d'Andorre ou lorsque l'ANC-AD a informé l'entité qui ne dispose pas d'établissements dans la Principauté d'Andorre de ses obligations conformément aux dispositions de la présente Loi
 - b) Le défaut d'adoption de mesures pour remédier aux déficiences détectées, conformément aux dispositions de l'article 23.3.b) et de l'article 24.3.b), lorsque ces déficiences entraînent des vulnérabilités à des incidents ayant des effets perturbateurs importants sur un ou plusieurs services essentiels ou importants, et que l'entité n'a pas donné suite aux injonctions émises par l'autorité nationale compétente antérieurement à la survenance de l'incident.
 - c) Le manquement réitéré à l'obligation de notifier les incidents ayant des effets perturbateurs importants sur le service conformément aux dispositions de l'article 15. Le manquement est considéré comme réitéré à partir du deuxième manquement.
 - d) Le fait de ne pas adopter les mesures nécessaires pour résoudre les incidents conformément aux dispositions de l'article 14 lorsque ceux-ci ont un effet perturbateur important sur la prestation de services essentiels ou de services importants dans la Principauté d'Andorre ou dans d'autres pays.
3. Constituent des infractions graves :
 - a) Le manquement aux autres obligations que la présente Loi établit pour les entités essentielles ou importantes, qui ne sont pas qualifiées d'infractions très graves ni légères conformément aux dispositions du présent article. Sont exemptées les entités essentielles et importantes qui ne disposent pas d'un établissement dans la Principauté d'Andorre,

tant que l'ANC-AD ne leur a pas notifié leur qualité d'entité essentielle ou importante pour la Principauté d'Andorre et les obligations qui leur sont applicables conformément à la présente Loi.

- b) Le manquement aux dispositions réglementaires ou aux instructions techniques de sécurité émises par l'autorité nationale compétente concernée sur les précautions minimales que les entités essentielles ou importantes doivent adopter pour garantir la sécurité des infrastructures critiques, des réseaux et des systèmes d'information nécessaires pour fournir lesdits services.

4. Constituent des infractions légères :

- a) Le manquement aux dispositions réglementaires ou aux instructions techniques de sécurité émises par l'autorité nationale compétente en vertu de la présente Loi, lorsqu'il ne constitue pas une infraction grave.
- b) Le fait de ne pas compléter les informations que doit réunir la notification d'incidents compte tenu des dispositions de l'article 15.1, ou, le cas échéant, de ne pas transmettre le rapport justificatif sur l'impossibilité de réunir les informations prévues audit article.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 35. Infractions entraînant une violation de la sécurité des données personnelles

1. Lorsque l'autorité nationale compétente concernée dispose d'indices que le manquement aux obligations établies dans la présente Loi, commis par une entité essentielle ou importante, entraîne une violation de la sécurité des données personnelles, et que, par conséquent, il doit être notifié conformément aux dispositions de l'article 27.3, elle doit en informer l'APDA, dans un délai raisonnable.
2. Si l'APDA décide d'exercer ses pouvoirs et d'infliger une amende administrative, l'ANC-AD ne doit pas infliger d'amende administrative pour la même infraction. Toutefois, l'autorité nationale compétente concernée peut appliquer les mesures ou pouvoirs prévus aux paragraphes 3 (sauf le point 3.j) et 4 de l'article 23 et aux paragraphes 3 (sauf le point 3.j) et 4 de l'article 24.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 36. Sanctions

1. Pour la commission des infractions définies à l'article 34, conformément aux principes d'effectivité, de proportionnalité et de dissuasion, les sanctions suivantes sont infligées, lesquelles sont applicables indépendamment du fait que l'entité contrevenante soit ou non une entité de l'administration publique :
 - a) Pour la commission d'infractions très graves, amende administrative de 30.001 euros à 100.000 euros.
 - b) Pour la commission d'infractions graves, amende administrative de 15.001 euros à 30.000 euros.
 - c) Pour la commission d'infractions légères, avertissement ou amende administrative de 500 euros à 15.000 euros.

2. Ces amendes doivent être infligées en tenant compte des circonstances de chaque cas individuel, à titre complémentaire ou en remplacement des mesures qui doivent être adoptées pour que cessent ou soient corrigés les effets de l'infraction. Pour la décision relative à l'imposition d'amendes administratives et à leur montant, doivent être pris en compte, dans chaque cas particulier et au minimum, les éléments prévus à l'article 37.
3. En outre, des astreintes peuvent être infligées pour obliger une entité essentielle ou importante à mettre fin à une infraction conformément à une décision préalable de l'ANC-AD.
4. Le montant recouvré en application des sanctions prévues dans la présente Loi est destiné à financer le budget propre de l'ANC-AD.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 37. Graduation des sanctions

L'autorité qui dispose du pouvoir de sanction doit graduer les sanctions prévues au présent Titre compte tenu des critères suivants :

- a) Le degré de culpabilité ou l'existence d'une intention.
- b) La continuité ou la persistance du comportement infractionnel.
- c) La nature et le montant des dommages et préjudices causés.
- d) La récidive, par la commission au cours de la dernière année de plus d'une infraction de même nature, lorsqu'elle a été déclarée par une décision définitive dans la voie administrative.
- e) Le nombre d'utilisateurs affectés.
- f) Le volume du chiffre d'affaires de l'entité contrevenante.
- g) L'utilisation par l'entité contrevenante de programmes de récompense pour la découverte de vulnérabilités dans les infrastructures critiques, les réseaux et les systèmes d'information, qu'ils soient propres ou de tiers, qui sont nécessaires à la prestation de ses services.
- h) Les actions réalisées par l'entité contrevenante pour pallier les effets ou les conséquences de l'infraction.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 38. Proportionnalité des sanctions

1. L'autorité qui dispose du pouvoir de sanction peut graduer le montant de la sanction en appliquant l'échelle relative à la catégorie d'infractions précédant en gravité celle dans laquelle s'inscrit l'infraction considérée dans le cas d'espèce lorsque se présentent les hypothèses suivantes :
 - a) Lorsqu'est constatée une diminution caractérisée de la culpabilité de l'entité contrevenante résultant de la réunion significative de plusieurs des critères énoncés à l'article 37.
 - b) Lorsque l'entité contrevenante a régularisé la situation irrégulière de manière diligente.
 - c) Lorsque l'entité contrevenante a reconnu spontanément sa culpabilité.
2. Compte tenu de la nature des faits et de la réunion significative des hypothèses indiquées au paragraphe précédent, l'autorité qui dispose du pouvoir de sanction peut ne pas décider l'ouverture de la procédure de sanction et procéder, à la place, à un avertissement à l'entité

contrevenante afin que, dans le délai que l'autorité qui dispose du pouvoir de sanction détermine, elle justifie l'adoption des mesures correctrices qui, dans chaque cas, sont pertinentes, pour autant que soient réunies les conditions suivantes :

- a) Que les faits soient constitutifs d'une infraction légère ou grave conformément aux dispositions de la présente Loi.
- b) Que l'entité contrevenante n'ait pas été sanctionnée ou n'ait pas fait l'objet d'un avertissement au cours des deux années précédentes pour la commission d'infractions prévues par la présente Loi. Si l'avertissement n'est pas suivi d'effet dans le délai déterminé par l'autorité, il est procédé à l'ouverture de la procédure de sanction correspondante en raison de ce manquement.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 39. Concours d'infractions

1. Il n'y a pas lieu d'imposer des sanctions conformément aux dispositions de la présente Loi lorsque les faits constitutifs de l'infraction le sont également d'une autre infraction prévue par la réglementation sectorielle à laquelle le prestataire du service est soumis et qu'il existe une identité du bien juridique protégé.
2. Si, à la suite d'une action de sanction, il est pris connaissance de faits susceptibles d'être constitutifs d'infractions prévues par d'autres lois, ceux-ci sont portés à la connaissance des organes ou organismes compétents pour leur supervision et leur sanction.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 40. Prescription des infractions

1. Les infractions se prescrivent dans les délais suivants :
 - a) Les infractions légères, au bout d'un an.
 - b) Les infractions graves, au bout de deux ans.
 - c) Les infractions très graves, au bout de trois ans.
2. Le début d'une activité d'inspection suspend le délai de prescription des infractions.
3. Le délai de prescription des infractions court à compter du jour où cesse l'action ou l'omission sanctionnable.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Article 41. Prescription des sanctions

Les sanctions pour infractions légères se prescrivent dans un délai d'un an, les sanctions pour infractions graves dans un délai de deux ans et les sanctions pour infractions très graves dans un délai de trois ans, à compter de la date de notification de la décision de sanction devenue définitive.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Disposition additionnelle première. Mission confiée au Gouvernement

Le Gouvernement est chargé, dans un délai maximal de dix-huit mois à compter de l'entrée en vigueur de la présente Loi, d'évaluer l'opportunité de constituer ou non une entité dotée de la personnalité juridique propre qui assume diverses fonctions en matière de numérisation, ou en rapport avec cette matière, y compris l'Agence nationale de cybersécurité de la Principauté d'Andorre (ANC-AD) et l'équipe de référence de réponse de la Principauté d'Andorre pour le traitement des incidents de cybersécurité (CSIRT-AD).

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Disposition finale première. Modification de la Loi 31/2021 , du 22 novembre, portant texte consolidé qualifiée de sécurité publique

1. Il est ajouté un paragraphe 3 à l'article 3 de la Loi 31/2021 , du 22 novembre, portant texte consolidé qualifiée de sécurité publique, modifiée par la Loi 4/2022 , du 31 janvier, du budget pour l'exercice 2022, qui est rédigé comme suit : « Article 3. Devoir de collaboration [...] »
3. De la même manière, aux mêmes fins, les autorités et les fonctionnaires compétents peuvent requérir l'aide et la collaboration de l'Agence de nationale de cybersécurité de la Principauté d'Andorre, ainsi que celle d'autres agences ou organismes de contrôle nationaux ou d'autres États dotés de pouvoirs similaires sur des domaines et des secteurs déterminés. »
2. L'article 27 de la Loi 31/2021 , du 22 novembre, portant texte consolidé qualifiée de sécurité publique, modifiée par la Loi 4/2022 , du 31 janvier, du budget pour l'exercice 2022, est modifié et est rédigé comme suit : « Article 27. Établissements et installations vulnérables Les armureries, les bijouteries, les entités bancaires, les entreprises de sécurité ou de vente de matériel de sécurité, ou tout autre établissement ou installation pouvant être considéré comme particulièrement vulnérable ou exposé en matière de sécurité, y compris les entités essentielles ou importantes considérées comme telles en vertu des dispositions de la législation en vigueur à chaque moment en matière de sécurité des réseaux et des systèmes d'information, doivent disposer des mesures de protection établies par voie réglementaire, afin de prévenir la commission d'actes délictueux contre ces établissements ou installations et les personnes qui y travaillent ou s'y trouvent, ou d'éviter qu'ils génèrent des risques pour ces personnes ou des tiers. »

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Disposition finale deuxième. Développement réglementaire

Le Gouvernement est autorisé à adopter les dispositions réglementaires nécessaires pour développer et appliquer la présente Loi.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Disposition finale troisième. Texte consolidé

Le Gouvernement est chargé, dans les termes prévus à l'article 116 du Règlement du Conseil général, de présenter au Conseil général, dans un délai maximal de six mois à compter de l'entrée en vigueur de la présente Loi, le projet de texte consolidé de la Loi 31/2021 , du 22 novembre, portant texte consolidé qualifiée de sécurité publique.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Disposition finale quatrième. Entrée en vigueur

1. La présente Loi entre en vigueur le lendemain de sa publication au Bulletin officiel de la Principauté d'Andorre.
2. Nonobstant les dispositions du paragraphe précédent, le chapitre troisième du Titre III et le Titre IV entrent en vigueur dans un délai de deux ans à compter de l'entrée en vigueur de la présente Loi.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Annexe 1. Entités essentielles

Secteur Sous-secteur Type d'entités

1. Énergie

- a) Infrastructures énergétiques Infrastructures énergétiques de sources renouvelables visées par le Décret du 16-05-2018 d'approbation et de publication du Plan sectoriel des infrastructures énergétiques d'Andorre. Infrastructures de production de chaleur centralisées visées par le Décret du 16-05-2018 d'approbation et de publication du Plan sectoriel des infrastructures énergétiques d'Andorre. Infrastructures de transport et de transformation d'énergie électrique visées par le Décret du 16-05-2018 d'approbation et de publication du Plan sectoriel des infrastructures énergétiques d'Andorre. Infrastructures de distribution d'énergie thermique visées par le Décret du 16-05-2018 d'approbation et de publication du Plan sectoriel des infrastructures énergétiques d'Andorre.
- b) Électricité Entité chargée de l'importation, de la production, de la distribution et de la commercialisation d'énergie électrique conformément à la Loi 5-2016, du 10 mars, qui régit l'organisme public Forces Elèctriques d'Andorra (FEDA) et le régime des activités des secteurs de l'électricité, du froid et de la chaleur. Entreprises productrices et distributrices d'électricité. Participants au marché de l'électricité qui fournissent des services de stockage de l'énergie, d'agrégation ou de participation active de la demande.
- c) Carburants Exploitants d'installations de production, de raffinage, de traitement, de stockage et/ou de transport de pétrole en vertu du Décret d'approbation du Règlement relatif au stockage, à l'approvisionnement, à la distribution et à l'utilisation des hydrocarbures, du 28 février 2018.
- d) Gaz Entreprises de fourniture, de distribution, de transmission et/ou systèmes de stockage en vertu de la Loi d'aménagement du secteur des gaz combustibles du 22-6-2000 du Décret d'approbation du Règlement relatif au stockage, à l'approvisionnement, à la distribution et à l'utilisation des gaz combustibles et de leurs modifications respectives.
- e) Chauffage urbain Entité chargée de l'importation, de la production, de la distribution et/ou de la commercialisation de chauffage urbain.
- f) Hydrogène Entité de production d'hydrogène, de stockage et/ou de transmission.

2. Transport

- a) Transports terrestres Responsables des compagnies de transports terrestres et/ou licences conformément à la Loi 4/2015, du 15 janvier, des transports routiers. Autorités pu-

bliques responsables de la planification, du contrôle ou de la gestion de la circulation. Exploitants de systèmes de transport intelligents. Prestataires de services de transport sanitaire conformément au Décret 74/2021, du 10 mars 2021.

b) Transports ferroviaires Gestionnaires d'infrastructures ferroviaires

c) Transports aériens Opérateurs compétents de transport d'aéronefs conformément au Décret du 24-02-2016 portant approbation du Règlement relatif aux aéronefs non habités, pilotés à distance et, en particulier, ceux qui ont une finalité publique et/ou commerciale. Autorité chargée de réglementer, de contrôler, d'ordonner et de vérifier les activités relatives à l'aviation civile à l'intérieur des frontières de la Principauté d'Andorre.

3. Entités financières Entités financières visées par la Loi 7/2013, du 9 mai, relative au régime juridique des entités opérationnelles du système financier andorran et autres dispositions régissant l'exercice des activités financières dans la Principauté d'Andorre et par la Loi 35/2010, du 3 juin, relative au régime d'autorisation pour la création de nouvelles entités opérationnelles du système financier andorran.

4. Marchés financiers Entités opérationnelles du système financier qui, conformément à la réglementation en vigueur à tout moment, sont autorisées à opérer dans la Principauté d'Andorre et satisfont aux conditions requises légales établies

5. Santé Établissements de soins de santé 1 Prestataires de services de santé au sens défini dans le Décret législatif du 30-5-2018 de publication du texte consolidé de la Loi 6/2014, du 24 avril, des services sociaux et sociosanitaires. Laboratoires de référence, entités qui réalisent des activités de recherche et de développement de médicaments, entités qui fabriquent des produits pharmaceutiques de base et des spécialités pharmaceutiques, entités qui fabriquent des dispositifs médicaux considérés comme essentiels dans des situations d'urgence de santé publique (« la liste des dispositifs médicaux essentiels peut être définie ou modifiée pendant l'urgence de santé publique »).

6. Eau

a) Eaux potables Responsables du captage, du traitement, de la distribution et de l'approvisionnement en eau destinée à la consommation humaine au sens de la Loi de police et de protection des eaux.

b) Eaux usées Entreprises de collecte, d'évacuation ou de traitement des eaux usées urbaines, domestiques et industrielles. Stations d'épuration des eaux usées prévues par le Décret du 25-2-2009 d'approbation de la procédure simplifiée d'autorisation des déversements d'eaux et d'ouverture de stations d'épuration des eaux usées.

c) Eaux de surface L'Administration chargée du maintien de l'état naturel des eaux de surface, en établissant un régime de protection et de contrôle des eaux prévu par la Loi de police et de protection des eaux.

7. Infrastructures numériques

- Fournisseurs de services DNS ;
- Registres des noms de domaine de premier niveau ;
- Fournisseurs de points d'échange Internet ;
- Fournisseurs de services d'informatique en nuage ;
- Fournisseurs de services de centres de données ;

- Fournisseurs de réseaux de diffusion de contenu ;
- Prestataires de services de confiance conformément à la Loi 9/2021 , du 29 avril, portant modification de la Loi 35/2014 , du 27 novembre, des services de confiance électronique ;
- Fournisseurs de réseaux publics de communications électroniques et fournisseurs de services de communications électroniques.

8. Administration publique Entités des administrations publiques du gouvernement central. Entités des administrations publiques des comuns ou d'autres niveaux organisationnels. I Y compris les centres de soins primaires, les centres sociosanitaires, les services sociaux, les hôpitaux et les cliniques privées.

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)

Annexe 2. Entités importantes

Secteur Sous-secteur Type d'entités

1. Gestion des déchets

- a) Gestionnaires Gestionnaires autorisés à réaliser des opérations de gestion des déchets, qu'ils soient ou non producteurs de déchets, prévus dans la Loi 25/2004 , du 14 décembre des déchets.
- b) Centre de transfert Centres chargés de conditionner et de stocker temporairement les déchets avant leur valorisation ou leur exportation, prévus dans la Loi 25/2004 , du 14 décembre des déchets.
- c) Déchetterie Centres de déchetterie communaux ou industriels, prévus dans la Loi 25/2004 , du 14 décembre des déchets.
- d) Centre de valorisation Centre de valorisation destiné exclusivement à la récupération totale ou partielle de déchets en vue de leur utilisation ultérieure, prévu dans la Loi 25/2004 , du 14 décembre des déchets.
- e) Centre de tri Centre destiné au stockage, au classement, à la sélection et/ou au conditionnement de déchets, qu'ils aient ou non été séparés préalablement sur le lieu même où ils ont été générés, en vue de leur valorisation ultérieure, prévu dans la Loi 25/2004 , du 14 décembre des déchets.
- f) Centre de transfert Centre de transfert qui conditionnent et stockent temporairement les déchets avant leur valorisation ou leur exportation, prévu dans la Loi 25/2004 , du 14 décembre des déchets.
- g) Installation de traitement thermique Unités techniques ou équipements, fixes ou mobilités, consacrées au traitement thermique de déchets, avec ou sans récupération de la chaleur produite par la combustion ; le site et l'installation complète, y compris toutes les lignes d'incinération, les installations de réception, de stockage et de prétraitement in situ des déchets ; les systèmes d'alimentation en déchets, en combustible et en air ; la chaudière ; les installations de traitement des gaz de combustion ; les installations de traitement in situ des résidus de l'incinération et des eaux usées ; la cheminée ; ainsi que les dispositifs et systèmes de contrôle des opérations d'incinération, d'enregistrement et de suivi des conditions d'incinération, prévus dans la Loi 25/2004 , du 14 décembre des déchets.

- h) Décharge Entité gestionnaire des installations d'élimination des déchets par leur dépôt contrôlé en surface ou sous terre, prévue dans la Loi 25/2004 , du 14 décembre des déchets.

2. Postes et messagerie Fournisseurs de services postaux et de messagerie.

3. Fabrication, production, distribution et commercialisation de produits chimiques Entités chargées de la fabrication de produits chimiques de base, de composés azotés, d'engrais, de matières plastiques et de caoutchouc synthétique sous formes primaires Entités chargées de la fabrication de pesticides et d'autres produits agrochimiques. Entités chargées de la fabrication d'autres produits chimiques tels que les explosifs, les colles, les huiles essentielles. Intermédiaires du commerce de combustibles, de minerais, de métaux et de produits chimiques industriels. Commerce de gros de produits chimiques.

4. Production alimentaire, transformation et distribution Entreprise publique ou privée qui, avec ou sans but lucratif, exerce toute activité liée à l'une quelconque des étapes de la production, de la transformation et de la distribution de denrées alimentaires.

5. Fabrication

- a) Fabrication de dispositifs médicaux, de diagnostic et de de diagnostic in vitro Entités consacrées à la fabrication de dispositifs médicaux, entendus comme tous les instruments, appareils, équipements, logiciels, implants, réactifs, matières ou autres articles destinés par le fabricant à être utilisés chez l'homme, seuls ou en association, pour l'une des fins médicales suivantes :

- Diagnostic, prévention, suivi, prédiction, pronostic, traitement ou atténuation d'une maladie.
- Diagnostic, suivi, traitement, atténuation ou compensation d'une blessure ou d'un handicap.
- Investigation, remplacement ou modification de l'anatomie ou d'un processus ou état physiologique ou pathologique.
- Obtention d'informations au moyen de l'examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus, et qui n'exerce pas son action principale prévue à l'intérieur ou à la surface du corps humain par des moyens pharmacologiques, immunologiques ou métaboliques, mais dont la fonction peut être assistée par de tels moyens. Sont également incluses les entités consacrées à la fabrication de dispositifs médicaux de diagnostic in vitro, entendus comme les produits qui, sans être en soi un dispositif médical, sont destinés par leur fabricant à être utilisés conjointement avec un ou plusieurs de ces produits, pour permettre spécifiquement que le ou les dispositifs médicaux puisse être utilisé conformément à sa destination prévue ou pour contribuer spécifiquement et directement à la fonctionnalité médicale des dispositifs médicaux au regard de leur destination prévue. Sont exclues les entités essentielles consacrées à la prestation de services de santé au sens exposé dans le Décret législatif du 30-5-2018 de publication du texte refondu de la Loi 6/2014 , du 24 avril, des services sociaux et socio-sanitaires mentionnées à l'Annexe I.

- b) Fabrication de produits informatiques, électroniques et de dispositifs optiques Entités consacrées à la fabrication d'ordinateurs, de périphériques d'ordinateur, d'équipements de communication et de produits électroniques, ainsi qu'à la fabrication de composants

pour ces produits. Sont également réputées incluses les entités consacrées à la fabrication de produits électroniques grand public, d'équipements de mesure, d'essai et de navigation, d'équipements d'irradiation, électromédicaux et électrothérapeutiques instruments et équipements optiques, ainsi qu'à la fabrication de supports magnétiques et optiques.

- c) Fabrication d'équipements électriques Entités consacrées à la fabrication de produits qui génèrent, distribuent et utilisent l'énergie électrique ainsi que celles consacrées à l'éclairage électrique, à la fabrication d'équipements de signalisation ou d'appareils électroménagers. Sont exclues les entités consacrées à la fabrication de produits informatiques, électroniques et de dispositifs optiques visées à l'Annexe II b.
- d) Fabrication de machines et d'équipements agissant de manière indépendante sur des matériaux Entités consacrées à la fabrication de machines et d'équipements qui agissent de manière indépendante sur les matériaux, que ce soit mécaniquement ou thermiquement, ou qui effectuent des opérations sur les matériaux (telles que la manutention, la pulvérisation, le pesage ou le conditionnement), y compris les composants mécaniques qui produisent et appliquent une force, ainsi que toute pièce primaire fabriquée spécialement à ces fins. De même, sont incluses les entités consacrées à la fabrication de dispositifs fixes et mobiles ou portatifs, qu'ils soient conçus pour un usage industriel, de construction et de génie civil, agricole ou domestique. et le génie civil, l'agriculture ou le foyer et les entités consacrées à la fabrication d'équipements spéciaux pour le transport de personnes ou de marchandises. Sont également incluses les entités consacrées à la fabrication d'autres machines à usage spécifique, utilisées ou non dans un processus de fabrication, telles que les équipements d'attractions foraines, les équipements automatiques de piste de quilles de quilles, etc. Sont exclues les entités consacrées à la fabrication de produits métalliques d'usage général, de dispositifs de commande associés, d'équipements informatiques, d'équipements de mesure et d'essai, des appareils de distribution et de commande d'électricité et de véhicules à moteur d'usage général.
- e) Fabrication de véhicules à moteur, de remorques y de semi-remorques Entités consacrées à la fabrication de véhicules à moteur pour le transport de passagers ou de marchandises, y compris la fabrication de leurs pièces et accessoires, ainsi que la fabrication de remorques et de semi-remorques. Sont exclus l'entretien et la réparation de ces véhicules.
- f) Fabrication d'autres matériels de transport Entités consacrées à la fabrication d'équipements de transport, telles que la construction de navires et la fabrication de matériel roulant ferroviaire et de locomotives, d'aéronefs et d'engins spatiaux, ainsi que la fabrication de leurs pièces.

6. Fournisseurs de services numériques

- Fournisseurs de places de marché en ligne
- Fournisseurs de moteurs de recherche en ligne
- Fournisseurs de plateformes de services de réseaux sociaux

Redacció vigent des del 23/06/2022 · text original · [Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació](#) (BOPA 2022-06-22)