Décret n° 2-21-406 du 4 hija 1442 (15 juillet 2021) pris pour l'application de la loi n° 05-20 relative à la cybersécurité

LE CHEF DU GOUVERNEMENT,

Vu le dahir n° 1-17-08 du 21 rejeb 1438 (19 avril 2017) portant délégation de pouvoir en matière d'administration de la défense nationale ;

Vu la loi n° 05-20 relative à la cybersécurité promulguée par le dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) ;

Vu le décret n° 2-82-673 du 28 rabii I 1403 (13 janvier 1983) relatif à l'organisation de l'administration de la défense nationale, tel qu'il a été modifié notamment par le décret n° 2-11-509 du 22 chaoual 1432 (21 septembre 2011) ;

Après délibération en Conseil du gouvernement, réuni le 16 kaada 1442 (27 juin 2021) ;

Après délibération en Conseil des ministres, réuni le 17 kaada 1442 (28 juin 2021),

DÉCRÈTE :

Chapitre premier

Des organes de gouvernance de la cybersécurité

Section première. – **De l'autorité nationale de la cybersécurité**

ARTICLE PREMIER. – On entend par autorité nationale de la cybersécurité au sens de la loi n° 05-20 susvisée, la direction générale de la sécurité des systèmes d'information relevant de l'administration de la défense nationale et désignée ci-après par « autorité nationale ».

Section 2. – **Du comité stratégique de la cybersécurité**

ART. 2. – Le comité stratégique de la cybersécurité, prévu à l'article 35 de la loi précitée n° 05-20, est présidé par le ministre délégué auprès du Chef du gouvernement, chargé de l'administration de la défense nationale, il se compose des membres ci-après :

– le ministre chargé de l'intérieur ;

– le ministre chargé des affaires étrangères ;

– le ministre chargé de l'économie et des finances ;

– le ministre chargé de l'industrie et de l'économie numérique ;

– l'inspecteur général des Forces armées royales ;

– le commandant de la gendarmerie royale ;

– le directeur général d'études et de documentation ;

– le directeur général de la sûreté nationale ;

– le chef du 5ème bureau de l'état-major général des Forces armées royales ;

– l'inspecteur des transmissions des Forces armées royales ;

– le directeur général de la surveillance du territoire ;

– le directeur général de la sécurité des systèmes d'information ;

– le directeur général de l'agence nationale de réglementation des télécommunications ;

– le directeur général de l'agence de développement du digital.

En cas d'absence ou d'empêchement, les ministres précités peuvent se faire représenter par les secrétaires généraux de leurs départements et les responsables des autres organismes par leurs adjoints directs.

Le président du comité stratégique de la cybersécurité peut inviter toute personne ou organisme dont il juge la participation utile pour assister aux travaux du comité.

ART. 3. – Le comité stratégique de la cybersécurité se réunit à la demande de son président, au moins une fois par an, conformément à un ordre du jour qu'il établit.

En cas d'urgence ou à la demande de son président ou de l'un des membres, le président peut également décider de la tenue de réunions exceptionnelles.

ART. 4. – Le secrétariat du comité stratégique de la cybersécurité est assuré par la direction générale de la sécurité des systèmes d'information.

A cet effet, ledit secrétariat est chargé, sous la supervision du président du comité stratégique de la cybersécurité, d'organiser les réunions dudit comité, d'en préparer l'ordre du jour, d'en faire le compte-rendu et d'assurer le suivi de l'exécution de ses décisions.

ART. 5. – Le comité stratégique de la cybersécurité établit son règlement intérieur fixant les modalités de son fonctionnement. Ce règlement est adopté lors de la première réunion dudit comité.

Le comité stratégique de la cybersécurité peut créer en son sein, tout autre comité qu'il estime nécessaire à l'accomplissement de ses missions.

Section 3. – **Du comité de gestion des crises et événements cybernétiques majeurs**

ART. 6. – En application des dispositions du troisième alinéa de l'article 36 de la loi précitée n° 05-20, le comité de gestion des crises et événements cybernétiques majeurs, présidé par la direction générale de la sécurité des systèmes d'information, se compose des représentants des autorités et organismes ci-après :

– l'autorité gouvernementale chargée de l'intérieur ;

– l'inspection générale des Forces armées royales ;

– la gendarmerie royale ;

– la direction générale d'études et de documentation ;

– la direction générale de la sûreté nationale ;

– la direction générale de la surveillance du territoire ;

– le 5ème bureau de l'état-major général des Forces armées royales ;

– l'inspection des transmissions des Forces armées royales.

Les autorités et organismes précités désignent leurs représentants permanents ainsi que leurs suppléants.

Le président du comité de gestion des crises et événements cybernétiques majeurs peut inviter toute personne ou organisme dont il juge la participation utile.

ART. 7. – Le comité de gestion des crises et événements cybernétiques majeurs prépare des rapports sur ses travaux et les transmet au comité stratégique de la cybersécurité.

ART. 8. – En application du troisième alinéa de l'article 36 de la loi précitée n° 05-20, le comité de gestion des crises et événements cybernétiques majeurs élabore un cadre de gestion des crises et événements cybernétiques majeurs et le soumet au comité stratégique de la cybersécurité pour approbation.

Le cadre de gestion précité doit définir notamment le champ d'intervention de chacun des membres du comité de gestion des crises et événements cybernétiques majeurs, ainsi que les procédures de gestion des crises et les modalités de communication et d'échange d'informations.

Chacun des membres du comité de gestion des crises et événements cybernétiques majeurs est chargé, dans la limite des prérogatives de l'autorité ou de l'organisme dont il relève, de l'enclenchement et du suivi des actions décidées par ledit comité.

Chapitre II

Du dispositif de sécurité des systèmes d'information

Section première. – **Dispositions propres aux entités et aux infrastructures d'importance vitale disposant de systèmes d'information sensibles**

Sous-section première. – De la directive nationale de la sécurité des systèmes d'information

ART. 9. – Dans le cadre des directives édictées par l'autorité nationale prévues au premier alinéa de l'article 4 de la loi n°05-20 susvisée, l'autorité nationale fixe par décision une directive nationale de la sécurité des systèmes d'information, qui détermine notamment les règles organisationnelles et techniques de sécurité des systèmes d'information. La directive nationale est publiée sur le site Internet de l'autorité nationale.

Sous-section 2. – Du référentiel de la classification des actifs informationnels et des systèmes d'information

ART. 10. – En application des articles 5 et 14 de la loi précitée n° 05-20, les entités et les infrastructures d'importance vitale classifient leurs systèmes d'information en se basant sur une analyse des impacts des incidents susceptibles de porter atteinte à la confidentialité, à la disponibilité ou à l'intégrité des actifs informationnels, consistant en toute ressource tel que le matériel, le logiciel, la donnée ou la procédure, qui composent les systèmes d'information précités.

ART. 11. – Afin d'effectuer la classification prévue à l'article 10 ci-dessus, chaque entité et infrastructure d'importance vitale réalisent une analyse des impacts des incidents de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité de leurs actifs informationnels.

Le niveau d'impact des incidents précités doit refléter l'importance des conséquences pouvant se traduire par l'incapacité de l'entité ou de l'infrastructure d'importance vitale à :

– accomplir ses missions ;

– préserver la vie, la santé ou le bien-être des personnes ;

– se conformer aux lois, aux règlements et aux obligations contractuelles ;

– préserver son image de marque et celle de l'Etat ;

– maintenir et renforcer la confiance des citoyens et des partenaires à l'égard des services offerts,

ou par la capacité de ladite entité ou infrastructure d'importance vitale à affecter le fonctionnement d'entités tierces, tributaires de ses services.

L'analyse des impacts doit se faire selon l'échelle suivante :

1. – Impact très grave : si un incident de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif informationnel pourrait :

– nuire au maintien des capacités de sécurité et de défense de l'Etat ;

– porter préjudice aux intérêts stratégiques de l'Etat ;

– porter atteinte à la santé et à la sécurité de la population ;

– perturber ou nuire au fonctionnement de l'économie nationale ;

– engendrer une incapacité totale ou partielle de plusieurs infrastructures d'importance vitale à assurer leurs fonctions essentielles.

2. – Impact grave : si un incident de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif informationnel pourrait engendrer :

– une incapacité totale ou partielle d'une infrastructure d'importance vitale à assurer ses fonctions essentielles ;

– une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions essentielles ;

– des pertes financières importantes pour une ou plusieurs entités ou infrastructures d'importance vitale.

3. – Impact modéré : si un incident de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif informationnel pourrait engendrer :

– une gêne ou perturbation mineure dans les fonctions d'une infrastructure d'importance vitale ;

– une incapacité partielle d'une ou de plusieurs entités non considérées comme infrastructures d'importance vitale, à assurer leurs fonctions ;

– des pertes financières modérées ;

– ou toute autre conséquence de nature analogue.

4. – Impact limité : si un incident de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité d'un actif informationnel pourrait causer :

– une gêne ou perturbation dans les fonctions d'une entité non considérée comme infrastructure d'importance vitale ;

– des pertes financières limitées ;

– ou toute autre conséquence de nature analogue.

ART. 12. – Un système d'information est classifié sur la base de l'échelle de l'analyse des impacts prévue à l'article 11 ci-dessus et ce, selon les niveaux suivants :

– « CLASSE A », si au minimum un incident de cybersécurité, portant sur la confidentialité, la disponibilité ou l'intégrité d'un des actifs informationnels qui compose le système d'information, a un impact très grave ;

– « CLASSE B », si tous les incidents de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs informationnels qui composent le système, ont au maximum un impact grave ;

– « CLASSE C », si tous les incidents de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs informationnels qui composent le système, ont au maximum un impact modéré ;

– « CLASSE D », si tous les incidents de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité, des actifs informationnels qui composent le système, ont au maximum un impact limité.

Sont réputés systèmes d'information sensibles, les systèmes d'information appartenant aux « CLASSE A » ou « CLASSE B ».

Chaque entité au sens de la loi n° 05-20 précitée, doit déclarer ses systèmes d'information sensibles à l'autorité nationale.

ART. 13. – Les actifs informationnels de type « données » classifiés sur la base de l'échelle de l'analyse des impacts prévue à l'article 11 ci-dessus sont classés suivant leur degré de sensibilité en termes de confidentialité selon les niveaux ci-après :

– « TRES SECRET », si un incident de cybersécurité portant sur la confidentialité a un impact très grave ;

– « SECRET », si un incident de cybersécurité portant sur la confidentialité a un impact grave ;

– « CONFIDENTIEL », si un incident de cybersécurité portant sur la confidentialité a un impact modéré ;

– « DIFFUSION RESTREINTE », si un incident de cybersécurité portant sur la confidentialité a un impact limité.

Pour l'application des dispositions de l'article 11 de la loi précitée n° 05-20, les données classifiées appartenant à l'un des niveaux « TRES SECRET » et « SECRET » sont considérées des données sensibles.

ART. 14. – Chaque entité ou infrastructure d'importance vitale applique les mesures de protection relatives à la sécurité des systèmes d'information proportionnellement à la classification attribuée. Ces mesures portent notamment sur :

– le marquage, traitement, stockage et transit et de destruction des informations et supports ;

– les consignes de sécurité à respecter par les personnes ;

– la sécurité physique.

L'autorité nationale édicte les référentiels et guides relatifs à ces mesures de protection, en tenant compte des différents niveaux de classification des systèmes d'information et des données.

ART. 15. – Chaque entité ou infrastructure d'importance vitale procède à la révision de la classification de ses actifs informationnels ou systèmes d'information au moins une fois tous les trois (3) ans et à chaque fois que nécessaire.

ART. 16. – Chaque entité ou infrastructure d'importance vitale informe et sensibilise son personnel sur les procédures de manipulation des actifs informationnels et des systèmes d'information selon leur classification et sur les mesures de protection qui leur sont applicables.

Sous-section 3. – Des missions du responsable de la sécurité des systèmes d'information

ART. 17. – Pour l'application du premier alinéa de l'article 6 de la loi n° 05-20 susvisée, chaque entité ou infrastructure d'importance vitale informe l'autorité nationale de son responsable de la sécurité des systèmes d'information, qui est chargé notamment de :

– identifier et analyser les enjeux et les risques de cybersécurité en tenant compte des évolutions réglementaires et techniques ;

– définir les objectifs de cybersécurité en collaboration avec les parties prenantes et élaborer les mesures de sécurité appropriées ;

– participer à l'élaboration et au suivi de la politique de sécurité des systèmes d'information en collaboration avec les parties prenantes ;

– définir pour la mise en œuvre de la politique de sécurité des systèmes d'information un plan d'actions annuel ou pluriannuel ;

– assurer le suivi de la gestion des incidents de cybersécurité ;

– rapporter régulièrement à sa hiérarchie les risques de sécurité des systèmes d'information ;

– animer des sessions de sensibilisation au profit du personnel.

Section 2. – **De la liste des secteurs d'activités d'importance vitale**

ART. 18. – La liste des secteurs d'activités d'importance vitale et les autorités gouvernementales, établissements publics ou autres personnes morales de droit public assurant la coordination de ces secteurs, est fixée dans l'annexe n°1 du présent décret.

La liste précitée peut être modifiée ou complétée par arrêté du Chef du gouvernement sur proposition de l'administration de la défense nationale.

Section 3. – **Des dispositions propres aux opérateurs**

ART. 19. – Pour l'application des dispositions du deuxième alinéa de l'article 28 de la loi n° 05-20 précitée, l'opérateur :

– désigne un point focal pour faciliter l'accès aux installations de l'opérateur et apporter le concours nécessaire pour l'installation des dispositifs techniques sur ses réseaux ;

– fournit les éléments de l'architecture de ses réseaux permettant de déterminer l'emplacement du déploiement de ces dispositifs ainsi que leurs spécifications techniques ;

– fournit les prérequis techniques pour la connexion des dispositifs précités avec les points du réseau de l'opérateur fixés par l'autorité nationale ;

– permet de déployer les dispositifs techniques dans un environnement sécurisé ;

– assiste l'autorité nationale à l'installation des dispositifs techniques permettant le recueil et l'analyse des données techniques, conformément aux dispositions de l'article 28 de la loi précitée n° 05-20 ;

– limite l'accès à ces dispositifs aux seules personnes désignées à cet effet par l'autorité nationale ;

– permet à l'autorité nationale d'administrer et d'exploiter à distance les dispositifs techniques, et de les tester périodiquement pour en garantir l'efficience lors d'un incident de cybersécurité.

Ces dispositifs ne doivent pas nuire à la disponibilité, à la sécurité et à l'intégrité des réseaux et services fournis par l'opérateur.

Chapitre III

Des critères de qualification des prestataires d'audit de la sécurité des systèmes d'information, des modalités de déroulement de l'audit et des critères de qualification des prestataires de services de cybersécurité

Section première. – **Des critères de qualification des prestataires d'audit**

ART. 20. – La qualification des prestataires d'audit de la sécurité des systèmes d'information est soumise aux critères ci-après :

– être constitué sous forme de société de droit marocain ;

– avoir une expertise dans l'audit de la sécurité des systèmes d'information ;

– avoir une structure organisationnelle dédiée exclusivement à l'audit de la sécurité des systèmes d'information ;

– remplir les conditions figurant dans le référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information prévu par l'article 22 ci-dessous ;

– être qualifié au minimum dans trois (3) domaines d'audit parmi ceux prévus dans l'annexe 2 du présent décret et disposer d'un auditeur au minimum par domaine de qualification demandé.

En outre, le prestataire d'audit doit, afin de fournir des prestations d'audit de la sécurité des systèmes d'informations ayant la classification « CLASSE A » prévue à l'article 12 du présent décret, remplir les conditions suivantes :

– le capital de la société doit être détenu majoritairement par des marocains ;

– les auditeurs proposés doivent être de nationalité marocaine.

ART. 21. – La demande de qualification est déposée par le prestataire d'audit de la sécurité des systèmes d'information auprès de l'autorité nationale, accompagnée d'un dossier comportant les documents suivants :

– copie des statuts de la société ;

– attestation d'inscription au registre de commerce ;

– liste des noms des associés et leurs nationalités ;

– copies des pièces d'identité des dirigeants de la société et ses organes d'administration ainsi que des auditeurs proposés ;

– note indiquant les moyens humains et techniques de la société ;

– copies des casiers judiciaires des auditeurs proposés ;

– *curriculums vitae* des auditeurs proposés et le cas échéant les copies de leurs diplômes et certificats de formation ;

– copies des contrats de travail conclus avec les auditeurs proposés ;

– copies des attestations délivrées par les maîtres d'ouvrages au profit desquels ont été exécutées des prestations d'audit de la sécurité des systèmes d'information, et devant préciser notamment la nature de la prestation fournie et la date de sa réalisation ;

– document décrivant la méthodologie appliquée pour conduire la prestation d'audit, objet de la demande de qualification.

Le prestataire d'audit de la sécurité des systèmes d'information doit informer l'autorité nationale de toute modification de l'un des éléments figurant dans le dossier de la demande de qualification.

ART. 22. – Après s'être assuré que le dossier de la demande comprend tous les documents et informations requis, l'autorité nationale soumet le prestataire d'audit de la sécurité des systèmes d'information, à ses frais, à une évaluation des prestations objet de la demande par l'un des organismes qu'elle désigne à cet effet.

L'évaluation précitée s'effectue conformément au référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information élaboré par l'autorité nationale et publié sur son site Internet. Ledit référentiel précise notamment les modalités d'évaluation des auditeurs ainsi que les niveaux de qualification.

ART. 23. – Au vu des résultats de l'évaluation prévue à l'article 22 ci-dessus, l'autorité nationale peut prendre la décision de qualification qui indique notamment :

– la dénomination et l'adresse du siège social du prestataire d'audit ;

– les domaines d'audit objet de la qualification, en indiquant que le prestataire peut auditer les systèmes d'information sensibles de «CLASSE A» ou de «CLASSE B» ;

– la durée de sa validité qui ne dépasse pas trois (3) ans ;

– la liste des auditeurs par domaines d'audit en indiquant leurs niveaux de qualification.

En cas de refus, l'autorité nationale notifie sa décision au demandeur de la qualification.

ART. 24. – Le renouvellement de la qualification du prestataire d'audit de la sécurité des systèmes d'information a lieu selon les mêmes conditions exigées pour son obtention, sous réserve du dépôt de la demande de renouvellement dans les soixante (60) jours, au moins, avant la date d'expiration de la décision de qualification.

ART. 25. – Le prestataire d'audit de la sécurité des systèmes d'information informe, sans délai, l'autorité nationale de toute modification intervenue dans l'un des éléments sur la base desquels la qualification a été délivrée.

ART. 26. – Si le prestataire d'audit qualifié ne répond plus à l'un des critères sur la base desquels la qualification lui a été délivrée, l'autorité nationale le met en demeure de se conformer aux prescriptions y afférentes dans un délai qu'elle fixe selon l'importance de ses prescriptions.

Si le prestataire d'audit ne défère pas à la mise en demeure, l'autorité nationale suspend sa qualification, jusqu'à ce qu'il se conforme auxdites prescriptions, à défaut, la qualification est retirée.

ART. 27. – La liste des prestataires d'audit des systèmes d'information qualifiés est publiée au « Bulletin officiel » et sur le site Internet de l'autorité nationale.

Section 2. – **Des modalités de déroulement de l'audit de la sécurité des systèmes d'information sensibles réalisés par les prestataires d'audit qualifiés**

ART. 28. – Les entités et les infrastructures d'importance vitale procèdent à l'audit de la sécurité de leurs systèmes d'information sensibles selon les domaines fixés à l'annexe n° 2 du présent décret lorsque les systèmes d'information en question s'y prêtent, sous réserve que la fréquence de chaque audit portant sur un même domaine ne doit pas dépasser trois (3) ans.

ART. 29. – L'audit s'effectue en vertu d'un contrat conclu entre le commanditaire d'audit et le prestataire d'audit qualifié. Cet audit ne commence qu'après la tenue d'une réunion entre les représentants du prestataire d'audit et ceux de l'entité auditée au cours de laquelle ils s'accordent sur l'ensemble des aspects de l'audit et toutes les clauses du contrat précité qui doit faire apparaître notamment les mentions suivantes :

– l'objet, le périmètre, les lieux d'exécution et les modalités de l'audit ;

– les noms et les missions des auditeurs désignés par le prestataire ;

– les normes à appliquer pour réaliser l'audit ;

– les délais d'exécution de l'audit ;

– les canaux de communication sécurisés entre le prestataire et l'entité auditée et le cas échéant entre le prestataire et le commanditaire d'audit ;

– les moyens nécessaires à la réalisation de l'audit ;

– les clauses de confidentialité concernant l'audit.

ART. 30. – L'entité doit, préalablement à l'audit, communiquer au prestataire d'audit toute la documentation nécessaire à l'accomplissement de sa mission.

Le prestataire d'audit doit respecter, lors de l'accomplissement de ses missions, les exigences techniques par domaine d'audit spécifiées dans le référentiel d'exigences des prestataires d'audit visé à l'article 22 ci-dessus.

ART. 31. – Le prestataire d'audit doit informer immédiatement l'entité auditée de toute faille constatée présentant un risque imminent et significatif, et dans la mesure du possible, lui proposer les mesures permettant de lever ce risque.

Les constats d'audit, doivent être documentés, tracés, et conservés durant toute la durée de l'audit, par le prestataire d'audit à l'occasion de l'exercice de sa mission.

ART. 32. – A la fin de sa mission, le prestataire d'audit qualifié doit remettre au commanditaire d'audit le rapport final d'audit accompagné de tous les documents et supports y afférents.

Une réunion de clôture est organisée au cours de laquelle le prestataire présente au commanditaire d'audit et à l'entité auditée la synthèse du rapport d'audit et les recommandations y afférentes.

Au terme de sa mission, le prestataire ne doit garder aucune copie des rapports, documents et supports fournis.

ART. 33. – L'entité ou l'infrastructure d'importance vitale auditée conserve le rapport d'audit et les documents y afférents pendant une durée de trois (3) ans au moins.

Section 3. – **Des critères de qualification des prestataires de services de cybersécurité**

ART. 34. – En application des dispositions de l'article 25 de la loi précitée n° 05-20, la qualification d'un prestataire de services de cybersécurité porte sur le domaine de la détection des incidents de cybersécurité et/ou le domaine de l'analyse, l'investigation et le traitement des incidents de cybersécurité, selon les critères suivants :

– être constitué sous forme de société de droit marocain ;

– avoir une expertise dans la fourniture de prestations de cybersécurité ;

– avoir une structure organisationnelle et des moyens techniques dédiés exclusivement à la fourniture de prestations de cybersécurité ;

– compter parmi son personnel, un minimum de trois (3) spécialistes dans l'un des domaines d'activité de qualification précités, disposant de l'expérience et des qualifications nécessaires fixés dans le référentiel d'exigences des prestataires de services de cybersécurité, élaboré par l'autorité nationale et publié sur son site Internet ;

– garantir que l'hébergement et le traitement des données sensibles relatives aux services de détection et d'analyse des incidents de cybersécurité soient réalisés exclusivement sur le territoire national ;

– garantir que l'exploitation et l'administration des services de détection et d'analyse des incidents de cybersécurité soient réalisées exclusivement sur le territoire national.

En outre, le prestataire doit, afin de fournir des prestations de services de cybersécurité des systèmes d'information sensibles ayant la classification « CLASSE A », remplir les conditions suivantes :

– le capital de la société doit être détenu majoritairement par des marocains ;

– les spécialistes proposés doivent être de nationalité marocaine.

ART. 35. – La demande de qualification est déposée par le prestataire de services de cybersécurité auprès de l'autorité nationale accompagnée d'un dossier comportant les documents suivants :

– copie des statuts de la société ;

– attestation d'inscription au registre de commerce ;

– liste des noms des associés et leurs nationalités ;

– copies des pièces d'identité des dirigeants de la société et ses organes d'administration ainsi que des spécialistes proposés ;

– note indiquant les moyens humains et techniques de la société ;

– copies des casiers judiciaires des spécialistes proposés ;

– *curriculums vitae* des spécialistes et le cas échéant les copies de leurs diplômes et certificats de formation ;

– copies des contrats de travail conclus avec les spécialistes proposés ;

– copies des attestations délivrées par les maîtres d'ouvrages au profit desquels ont été exécutées des prestations de services de cybersécurité, et devant préciser notamment la nature de la prestation fournie et la date de sa réalisation ;

– document décrivant la méthodologie appliquée pour conduire la prestation de services de cybersécurité, objet de la demande de qualification.

Le prestataire de services de cybersécurité doit informer l'autorité nationale de toute modification de l'un des éléments figurant dans le dossier de la demande de qualification.

ART. 36. – Après s'être assuré que le dossier de la demande comprend tous les documents et informations requis, l'autorité nationale soumet le prestataire de services de cybersécurité, à ses frais, à une évaluation des prestations objet de la demande par l'un des organismes qu'elle désigne à cet effet.

L'évaluation précitée s'effectue conformément au référentiel d'exigences des prestataires de services de cybersécurité élaboré par l'autorité nationale et publié sur son site Internet.

ART. 37. – Au vu des résultats de l'évaluation prévue à l'article 36 ci-dessus, l'autorité nationale peut prendre la décision de qualification qui indique notamment :

– la dénomination et l'adresse du siège social du prestataire de services de cybersécurité ;

– les domaines objet de la qualification, en indiquant que le prestataire peut fournir des services de cybersécurité pour les systèmes d'information sensibles de «CLASSE A» ou de «CLASSE B» ;

– la durée de sa validité qui ne dépasse pas trois (3) ans ;

– la liste des spécialistes retenus par domaine de prestation de services de cybersécurité.

En cas de refus de la qualification, le demandeur doit être avisé par l'autorité nationale.

ART. 38. – Le renouvellement de la qualification du prestataire de services de cybersécurité a lieu selon les mêmes conditions exigées pour son obtention, sous réserve du dépôt de la demande de renouvèlement dans les soixante (60) jours, au moins, avant la date d'expiration de la décision de qualification.

ART. 39. – Le prestataire de services de cybersécurité informe, sans délai, l'autorité nationale de toute modification intervenue dans l'un des éléments sur la base desquels la qualification a été délivrée.

ART. 40. – Si le prestataire de services de cybersécurité ne répond plus à l'un des critères sur la base desquels la qualification lui a été délivrée, l'autorité nationale le met en demeure de se conformer aux prescriptions y afférentes dans un délai qu'elle fixe selon l'importance de ses prescriptions.

Si le prestataire de services de cybersécurité ne défère pas à la mise en demeure, l'autorité nationale suspend sa qualification, jusqu'à ce qu'il se conforme auxdites prescriptions, à défaut, la qualification est retirée.

ART. 41. – La liste des prestataires de services de cybersécurité qualifiés est publiée au «Bulletin officiel» et sur le site Internet de l'autorité nationale.

Chapitre IV

Des dispositions diverses, transitoires et finales

ART. 42. – L'autorité nationale élabore un référentiel de gestion des incidents de cybersécurité et le publie sur son site Internet. Ledit référentiel fixe notamment les modalités de déclaration et de traitement des incidents de cybersécurité.

ART. 43. – Les entités et les infrastructures d'importance vitale disposent d'un délai ne dépassant pas douze (12) mois, à compter de la date de publication du présent décret au « Bulletin officiel », pour classifier leurs systèmes d'information et déclarer ceux ayants un caractère sensible à l'autorité nationale, conformément aux dispositions de la loi précitée n° 05-20 et des textes pris pour son application.

ART. 44. – Les décisions d'homologation délivrées aux prestataires d'audit conformément aux dispositions de l'arrêté du Chef du gouvernement n° 3-44-18 du 21 safar 1440 (31 octobre 2018), fixant les critères d'homologation des prestataires d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale ainsi que les modalités de déroulement de l'audit, demeurent valables jusqu'à leur expiration.

ART. 45. – Sont abrogés :

– le décret n° 2-11-508 du 22 chaoual 1432 (21 septembre 2011) portant création du comité stratégique de la sécurité des systèmes d'information ;

– le décret n° 2-15-712 du 12 joumada II 1437 (22 mars 2016) fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale ;

– l'arrêté du Chef du gouvernement n° 3-44-18 du 21 safar 1440 (31 octobre 2018), fixant les critères d'homologation des prestataires d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale ainsi que les modalités de déroulement de l'audit.

ART. 46. – Le ministre délégué auprès du Chef du gouvernement, chargé de l'administration de la défense est chargé de l'exécution du présent décret qui sera publié au *Bulletin officiel*.

Fait à Rabat, le 4 hija 1442 (15 juillet 2021).

SAAD DINE EL OTMANI.

*

* *

ANNEXE 1

Liste des secteurs d'activités d'importance vitale et les autorités gouvernementales, établissements publics et personnes morales de droit public, assurant la coordination de ces secteurs

Secteurs d'activités d'importance vitale	Autorités gouvernementales, établissements publics et personnes morales de droit public, assurant la coordination de ces secteurs
Secteur de la sécurité publique	Autorité gouvernementale chargée de l'intérieur
Secteur des affaires étrangères	Autorité gouvernementale chargée des affaires étrangères
Secteur des finances	Autorité gouvernementale chargée des finances
Secteur de la législation	Secrétariat général du gouvernement
Secteur de l'agriculture	Autorité gouvernementale chargée de l'agriculture
Secteur de la santé	Autorité gouvernementale chargée de la santé
Secteurs de l'industrie, du commerce et de l'économie numérique	Autorité gouvernementale chargée de l'industrie, du commerce et de l'économie numérique
Secteur de la communication audiovisuelle	Autorité gouvernementale chargée de la communication
Secteur de la production et de la distribution de l'énergie	Autorité gouvernementale chargée de l'intérieur
	Autorité gouvernementale chargée de l'énergie
Secteur des mines	Autorité gouvernementale chargée des mines
Secteur des transports	Autorités gouvernementales chargées des transports
Secteur de la production et de la distribution d'eau	Autorités gouvernementales chargées de l'eau
Secteur bancaire	Bank Al-Maghrib
Secteur des télécommunications	Agence nationale de réglementation des télécommunications
Secteur des assurances et de la prévoyance sociale	Autorité de contrôle des assurances et de la prévoyance sociale

* * *

ANNEXE 2

Domaines d'audit objet de la qualification des prestataires d'audit de la sécurité des systèmes d'information

– **audit organisationnel et physique** : consiste à s'assurer que les politiques et procédures de sécurité définies et mises en place par l'entité auditée sont conformes aux directives de l'autorité nationale ;

– **audit d'architecture** : consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information, aux pratiques en vigueur, aux exigences de sécurité et aux règles internes de l'entité auditée ;

–**audit de configuration** : permet de vérifier la mise en œuvre de pratiques de sécurité conformes aux exigences et règles internes de l'entité auditée en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information ;

– **audit de code source** : consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une solution logicielle dans le but de s'assurer du respect des règles précises du codage ou d'analyser les vulnérabilités liées au développement ;

– **test d'intrusion** : permet d'évaluer la sécurité d'un système d'information ou d'un réseau en simulant les conditions réelles d'une attaque sur le système d'information. Ce test permet de découvrir des vulnérabilités sur le système d'information d'une entité auditée et de vérifier leur exploitabilité et leur impact sur l'entité ;

– **audit des systèmes industriels** : consiste en l'évaluation du niveau de sécurité d'un système industriel et des dispositifs de contrôle associés.

Le texte en langue arabe a été publié dans l'édition générale du « Bulletin officiel » n° 7011 du 29 hija 1442 (9 août 2021).