Legal Partners Advisors
الفـــاونية للـــشركـــاء المستشـــاريـــن
Tax & Legal

Newsletter

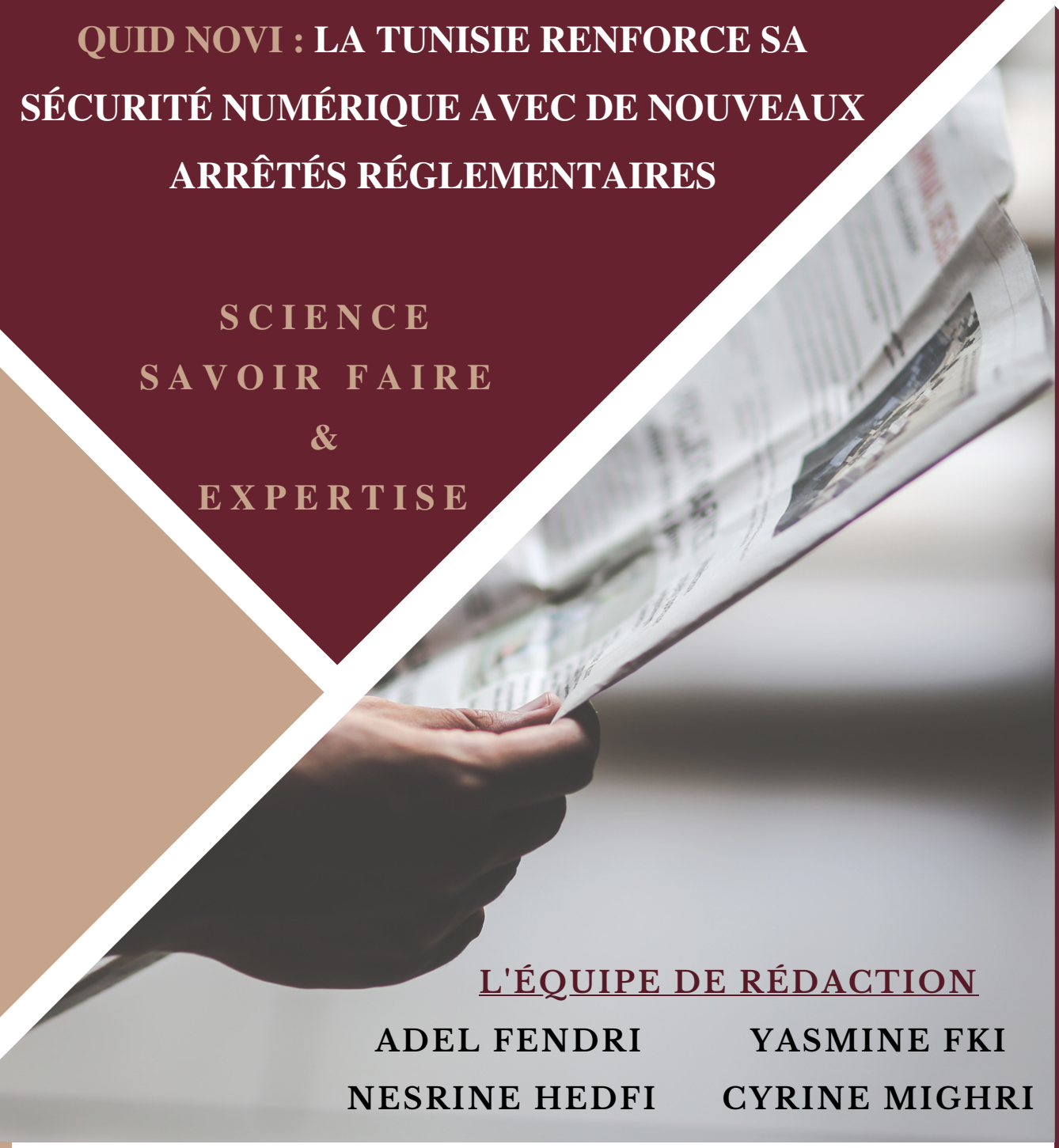
LPA JURI'SCOPE

Sept,22, 2023

N° 34

QUID NOVI : LA TUNISIE RENFORCE SA SÉCURITÉ NUMÉRIQUE AVEC DE NOUVEAUX ARRÊTÉS RÉGLEMENTAIRES

SCIENCE
SAVOIR FAIRE
&
EXPERTISE



L'ÉQUIPE DE RÉDACTION

ADEL FENDRI YASMINE FKI
NESRINE HEDFI CYRINE MIGHRI

WWW.LPA-LEGAL.COM.TN

https://www.linkedin.com/company/legal-partners-advisors/

https://www.facebook.com/profile.php?id=100089715340398

QUID NOVI: LA TUNISIE RENFORCE SA SÉCURITÉ NUMÉRIQUE AVEC DE NOUVEAUX ARRÊTÉS RÉGLEMENTAIRES

Dans un monde de plus en plus connecté et dépendant des technologies de l'information, la sécurité numérique est devenue une préoccupation majeure pour les nations du globe.

La Tunisie, consciente de l'importance cruciale de la protection de ses systèmes informatiques et de la confidentialité des données, a pris des mesures audacieuses pour renforcer sa posture de sécurité numérique.

Au cœur de ces mesures se trouvent trois arrêtés ministériels émis par le Ministère des Technologies de la Communication, tous datés du 12 septembre 2023, en conformité avec le décret-loi n° 2023-17 du 11 mars 2023 relatif à la cybersécurité.

Ces arrêtés marquent un tournant dans la manière dont la Tunisie aborde la sécurité numérique, en introduisant de nouvelles procédures, critères techniques et mécanismes de classification des organismes soumis à des audits obligatoires et périodiques de leurs systèmes d'information .

De plus, ils établissent des lignes directrices strictes pour l'octroi et le retrait du prestigieux label "sécurisé."

Cet article explore respectivement ces nouveaux arrêtés réglementaires:

- Arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les procédures et les mécanismes de classification des organismes soumis à un système d'audit obligatoire et périodique de leurs systèmes d'information (1)
- Arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit. (2)
- Arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les procédures et les conditions d'octroi du label « sécurisé » et de son retrait (3)
- Arrêté du ministre des technologies de la communication du 13 septembre 2023, fixant les procédures et les conditions d'octroi, de renouvellement et de retrait du label « Fournisseur de services informatiques en nuage gouvernemental (G-cloud) » et du label « Fournisseur de services informatiques en nuage national (N-cloud) » (4)

1. NOUVELLES PROCÉDURES DE CLASSIFICATION DES ORGANISMES POUR L'AUDIT DES SYSTÈMES D'INFORMATION

A. NOUVELLE CLASSIFICATION OBLIGATOIRE POUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

L'Agence Nationale de la Cybersécurité a mis en place de nouvelles procédures de classification des organismes en vertu du décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité.

Cette classification s'applique de manière obligatoire et périodique aux structures mentionnées à l'article 6 dudit décret-loi.

La classification repose sur le niveau de confiance numérique, qui est réparti en trois niveaux distincts :

1. **Premier niveau** : Les organismes classifiés au premier degré.
2. **Deuxième niveau**: Les organismes classifiés au deuxième degré.
3. **Troisième niveau** : Les organismes non classifiés.

CLASSIFICATION AU PREMIER NIVEAU

Les structures répondant aux critères suivants sont classées au premier niveau :

- Respect de l'obligation de l'audit obligatoire de la sécurité des systèmes d'information et mise en application des recommandations qui en découlent,
- Utilisation d'équipements et de solutions homologuées conformément à la législation en vigueur, selon une liste établie par l'Agence,
- Hébergement des logiciels, des plateformes électroniques et des infrastructures numériques en interne dans un cloud privé ou chez des fournisseurs de services cloud ayant un label "Fournisseur de services informatiques en nuage gouvernemental (Gcloud)" ou un label "Fournisseur de services informatiques en nuage national (N-cloud)".

CLASSIFICATION AU DEUXIÈME NIVEAU

Les structures répondant aux deux critères suivants sont classées au deuxième niveau :

- Respect de l'obligation de l'audit obligatoire de la sécurité des systèmes d'information, mais sans l'application entière ou partielle des recommandations qui en découlent,
- Utilisation d'équipements et de solutions homologuées conformément à la législation en vigueur, selon une liste établie par l'Agence.

CLASSIFICATION AU TROISIÈME NIVEAU

Les structures répondant aux critères suivants sont classées au premier niveau :

- Respect de l'obligation de l'audit obligatoire de la sécurité des systèmes d'information et mise en application des recommandations qui en découlent,
- Utilisation d'équipements et de solutions homologuées conformément à la législation en vigueur, selon une liste établie par l'Agence,
- Hébergement des logiciels, des plateformes électroniques et des infrastructures numériques en interne dans un cloud privé ou chez des fournisseurs de services cloud ayant un label "Fournisseur de services informatiques en nuage gouvernemental (Gcloud)" ou un label "Fournisseur de services informatiques en nuage national (N-cloud)".

B. CRÉATION DE LA COMMISSION TECHNIQUE

Au sein de l'Agence Nationale de la Cybersécurité, une commission technique a été créée pour assurer le classement des structures soumises à cette obligation de classification. Cette commission est présidée par le directeur général de l'Agence ou son représentant et est composée de représentants des entités suivantes :

- Ministère chargé des Technologies de la Communication
- Centre d'Etudes et de Recherche des Télécommunications
- Agence Nationale des Fréquences
- Agence Nationale de Certification Électronique
- Agence Technique des Télécommunications

La commission technique se réunit sur convocation de son président chaque fois que cela s'avère nécessaire pour déterminer les niveaux de classement. Pour qu'elle puisse se réunir légalement, la majorité de ses membres doit être présente. En outre, les avis de la commission sont émis à la majorité des voix des membres présents, avec la voix du président prépondérante en cas d'égalité.

Si le quorum n'est pas atteint lors de la première réunion, une deuxième réunion est convoquée trois (3) jours après la première date. Dans ce cas, la commission peut se réunir quel que soit le nombre de membres présents, et ses travaux sont consignés par des procès-verbaux. L'Agence nationale de la Cybersécurité assure le secrétariat permanent de cette commission.

2. NOUVEAUX CRITÈRES ET MODALITÉS D'AUDIT POUR LA GESTION DES RECOMMANDATIONS

A. AUDIT OBLIGATOIRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Conformément au décret-loi n° 2023-17 du 11 mars 2023 relatif à la cybersécurité, les organismes énumérés à l'article 6 de ce décret sont soumis à un système d'audit obligatoire et périodique de la sécurité de leurs systèmes d'information. Cet audit est effectué au moyen d'une mission d'évaluation sur site.

L'audit de sécurité des systèmes d'information est effectué en stricte conformité avec le référentiel établi par l'Agence Nationale de la Cybersécurité, qui englobe les éléments essentiels suivants :

1. Évaluation des aspects structurels, organisationnels et opérationnels de la sécurité des systèmes d'information.
3. Audit technique des composants du système d'information et vérification de leur résistance aux incidents cybernétiques.
2. Analyse et évaluation des risques cybernétiques, ainsi que la présentation d'un plan de traitement visant à éliminer ou réduire les conséquences des incidents cybernétiques.

B. RAPPORT D'AUDIT

L'expert chargé de l'audit remet à l'organisme audité un rapport d'audit portant son cachet et sa signature, élaboré en accord avec le modèle de rapport d'audit fourni par l'Agence. Ce rapport comprend principalement les éléments suivants :

1. Une description complète du système d'information, avec des justifications en cas d'exclusion de certains composants de l'audit.
2. La vérification de la mise en application des recommandations et des solutions de sécurité organisationnelles et techniques proposées pour remédier aux insuffisances relevées lors de l'audit précédent.
3. Une évaluation exhaustive de la sécurité du système d'information, accompagnée d'une analyse détaillée des lacunes organisationnelles et techniques relatives aux procédures et mécanismes de sécurité adoptés, ainsi qu'une évaluation des risques potentiels découlant de l'exploitation des failles découvertes.
4. Des recommandations et des solutions de sécurité organisationnelles et techniques proposées pour remédier aux insuffisances constatées.
5. Une copie des procès-verbaux des réunions de démarrage et de clôture de la mission d'audit.

C. ÉVALUATION DU RAPPORT D'AUDIT PAR L'AGENCE

L'Agence Nationale de la Cybersécurité étudie attentivement le rapport d'audit soumis et répond par acceptation ou refus. Elle se réserve également le droit de demander à l'organisme audité de fournir des informations ou des documents complémentaires, ainsi que d'effectuer un contrôle sur site si nécessaire.

D. REJET DU RAPPORT D'AUDIT

L'Agence peut rejeter le rapport d'audit dans les situations suivantes :

1.Non-conformité du rapport d'audit au modèle spécifié à l'article 2 du présent arrêté.

2. Évaluation non pertinente ou incomplète de la sécurité du système d'information.

3. Absence des recommandations et des solutions requises pour remédier aux lacunes identifiées.

4. Non-respect du référentiel d'audit énoncé à l'article premier de cet arrêté.

En cas de rejet du rapport, l'organisme concerné est tenu de réaliser un nouvel audit et de soumettre ce nouveau rapport à l'Agence dans un délai ne dépassant pas deux mois à partir de la date de la notification.

E. SIGNALEMENT DE RISQUES DE SÉCURITÉ

L'expert auditeur est tenu d'informer immédiatement l'Agence lorsqu'il découvre des risques graves pour la sécurité du cyberespace. De plus, il est également tenu d'alerter l'organisme audité afin que des contre-mesures appropriées puissent être prises.

3. LE LABEL 'SÉCURISÉ' : NOUVELLES PROCÉDURES ET CONDITIONS

L'Agence Nationale de la Cybersécurité est habilitée, sur demande du développeur ou de l'importateur, à attribuer le label "sécurisé" à tout logiciel ou équipement électronique remplissant **les conditions suivantes** :

1. Conditions de sécurité et garanties adéquates pour protéger les utilisateurs et les données traitées, transmises et stockées contre les cyber-incidents.

2. Exemption de vulnérabilités de sécurité connues.

3. Assurance de la continuité du service, de la sûreté et de la qualité du fonctionnement, même dans des conditions d'utilisation inhabituelles et extrêmes.

A. PROCÉDURE DE DEMANDE DU LABEL "SÉCURISÉ"

Tout développeur ou importateur de logiciel ou d'équipement électronique désireux d'obtenir le label "sécurisé" doit soumettre une demande à l'Agence Nationale de la Cybersécurité. Cette demande peut être adressée par lettre recommandée, par voie électronique avec accusé de réception, ou directement à l'Agence sous pli fermé contre récépissé de dépôt.

La demande doit impérativement contenir les éléments suivants :

1. Une fiche signalétique, comportant le nom commercial ou l'identifiant descriptif du logiciel ou de l'équipement électronique, la date de production et le code de la version soumise à évaluation, ainsi que les domaines d'utilisation.

2. Des documents prouvant la propriété ou le droit de commercialisation ou d'exploitation au niveau national.

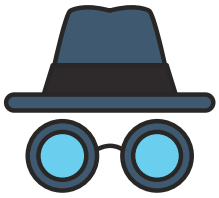
3. La charte professionnelle, disponible auprès des services de l'Agence, signée par le développeur ou l'importateur du logiciel ou de l'équipement électronique pour lequel le label "sécurisé" est demandé.

4. Une copie du logiciel ou un échantillon de l'appareil électronique soumis à évaluation.

5. Des documents décrivant les fonctions essentielles et les fonctionnalités de sécurité à évaluer.

6. Un rapport détaillé d'audit de sécurité rédigé par des experts-auditeurs exerçant conformément à la législation en vigueur. Ce rapport doit démontrer que le logiciel ou l'équipement électronique est exempt de vulnérabilités menaçant la sécurité des données, des utilisateurs et des systèmes associés, conformément au référentiel, à la méthodologie et aux normes techniques définies par l'Agence.

7. Une copie des certificats obtenus par le logiciel ou l'appareil électronique auprès de structures de certification nationales ou internationales compétentes, le cas échéant.



B. EXAMEN DES DEMANDES

Les demandes de label "sécurisé" sont examinées par une commission technique, présidée par le directeur général de l'ANCS ou son représentant. Cette commission est composée de membres du Centre d'Études et de Recherche des Télécommunications, de l'Agence Nationale des Fréquences, de l'Agence Nationale de Certification Électronique et de l'Agence Technique des Télécommunications.

La commission technique se réunit sur convocation de son président chaque fois que nécessaire pour étudier les demandes, émettre un avis sur les aspects techniques, et vérifier la conformité du logiciel ou de l'appareil électronique avec les textes juridiques et les guides de procédure relatifs à la cybersécurité.

La commission technique peut se réunir légalement en présence de la majorité de ses membres. Les avis sont émis à la majorité des voix des membres présents, avec la voix du président prépondérante en cas d'égalité. Si le quorum n'est pas atteint, une deuxième réunion est convoquée trois (3) jours après la première, et la commission peut alors se réunir quel que soit le nombre de membres présents, en consignant ses travaux par des procès-verbaux. L'ANCS assure le secrétariat permanent de cette commission.

C. ATTRIBUTION DU LABEL ET DURÉE DE VALIDITÉ

L'Agence accorde le label "sécurisé" dans un délai n'excédant pas un mois à partir de la date de la réunion de la commission technique. Le certificat de labélisation émis est valable pour une durée de trois (3) ans.

D.MISES À JOUR ET CONTRÔLE

Le développeur ou l'importateur est tenu d'informer l'Agence de toute modification apportée au logiciel ou à l'appareil électronique portant le label "sécurisé". Au surplus, L'Agence se réserve le droit de procéder à des contrôles réguliers du produit labélisé pour vérifier dans quelle mesure il continue de respecter les exigences de sécurité.

E. RETRAIT DU LABEL

L'Agence accorde le label "sécurisé" dans un délai n'excédant pas un mois à partir de la date de la réunion de la commission technique. Le certificat de labélisation émis est valable pour une durée de trois (3) ans.

L'Agence, sur proposition de la commission technique prévue à l'article 3 du présent arrêté, peut retirer le label "sécurisé" avant l'expiration de sa durée de validité dans les cas suivants :

1. Modification des caractéristiques techniques du logiciel ou de l'appareil électronique.

2. Évolution technologique introduisant des vulnérabilités critiques dans le logiciel ou l'équipement électronique.

Le développeur ou l'importateur sera notifié du retrait du label et devra prendre les mesures nécessaires pour remédier aux problèmes identifiés.

La labellisation ne pourra être réattribuée que lorsque les problèmes seront résolus et que le produit répondra à nouveau aux critères de sécurité requis.

4. LE LABEL 'SÉCURISÉ' : NOUVELLES PROCÉDURES ET CONDITIONS

L'arrêté du ministre des technologies de la communication du 13 septembre 2023, fixant les procédures et les conditions d'octroi, de renouvellement et de retrait du label « Fournisseur de services informatiques en nuage gouvernemental (G-cloud) » et du label « Fournisseur de services informatiques en nuage national (N-cloud) ». Met en évidence les critères d'attribution et de révocation des labels G-Cloud et N-Cloud, ainsi que les procédures associées.

A. CRITÈRES D'ATTRIBUTION ET DE RÉVOCATION DES LABELS G-CLOUD ET N-CLOUD

L'arrêté du ministre des technologies de la communication du 13 septembre 2023 est un document essentiel qui fixe les procédures et les conditions pour l'octroi, le renouvellement et le retrait des labels "Fournisseur de services informatiques en nuage gouvernemental (G-cloud)" et "Fournisseur de services informatiques en nuage national (N-cloud)" en Tunisie. Ces labels sont attribués aux prestataires de services d'hébergement qui s'engagent à respecter des normes strictes en matière de cybersécurité, de continuité d'activité et de qualité des services de cloud.

B. CATÉGORIES DE SERVICES DE CLOUD

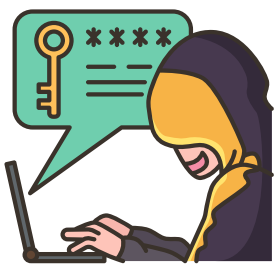
Le présent arrêté définit trois catégories de services de cloud que les fournisseurs peuvent proposer :

1. Logiciels en tant que service (SaaS) : Ce modèle implique la fourniture d'applications informatiques aux utilisateurs via un réseau de télécommunication.

2. Plateformes électroniques en tant que service (PaaS) : Il offre un environnement d'exploitation aux utilisateurs du cloud pour héberger et déployer leurs applications informatiques.

3. Infrastructures numériques en tant que service (IaaS) : Ce modèle fournit un espace sécurisé et les ressources cloud nécessaires pour héberger un centre de données, comprenant des serveurs, des unités de stockage et des équipements réseau.

Tous ces services sont hébergés dans des centres de données accessibles de manière sécurisée via un réseau de télécommunication public ou privé.



C. CRITÈRES D'ATTRIBUTION DU LABEL G-CLOUD

L'Agence Nationale de la Cybersécurité attribue le label "Fournisseur de services informatiques en nuage gouvernemental (G-cloud)" aux prestataires tunisiens, qu'ils appartiennent au secteur public ou privé, qui remplissent les conditions suivantes :

- Fournir au moins l'un des services informatiques en nuage mentionnés dans l'article 3 de l'arrêté.
- Être impérativement relié au réseau national intégré de l'administration et à la plateforme nationale d'interopérabilité.
- Utiliser des centres de données primaires et de secours situés en Tunisie.
- Conformité aux normes internationales en cybersécurité et continuité d'activité, conformément au référentiel établi par l'ANCS.
- Assurer un support technique 24 heures sur 24 et 7 jours sur 7 aux structures bénéficiaires des services cloud.

D. CRITÈRES D'ATTRIBUTION DU LABEL N-CLOUD

Le label "Fournisseur de services informatiques en nuage national (N-cloud)" est attribué aux prestataires tunisiens du secteur public ou privé qui remplissent les conditions suivantes :

- Fournir au moins l'un des services informatiques en nuage mentionnés dans l'article 3 de l'arrêté.
- Utiliser des centres de données primaires et de secours situés en Tunisie.
- Conformité aux normes internationales en cybersécurité et continuité d'activité, conformément au référentiel établi par l'ANCS.
- Assurer un support technique 24 heures sur 24 et 7 jours sur 7 aux structures bénéficiaires des services cloud.

E. PROCÉDURES D'ATTRIBUTION ET DE RÉVOCATION

Les demandes d'obtention des labels G-Cloud et N-Cloud, ainsi que les demandes de renouvellement, doivent être soumises à l'ANCS. Ces demandes doivent inclure des informations détaillées sur les centres de données, des documents légaux, des certificats de conformité en cybersécurité, des modèles de contrats de services, et d'autres éléments spécifiques.

Ces demandes sont examinées par une commission technique composée de représentants de diverses entités liées aux télécommunications et à la cybersécurité. La commission émet un avis sur l'attribution du label, qui est ensuite accordé par l'ANCS.

L'ANCS peut également effectuer des contrôles pour vérifier le respect des obligations par les détenteurs des labels et retirer ces labels en cas de non-conformité.

En résumé, cet arrêté vise à garantir la sécurité et la qualité des services de cloud en Tunisie en établissant des critères stricts d'attribution et de révocation des labels G-Cloud et N-Cloud, contribuant ainsi à renforcer la confiance dans les prestataires de services informatiques en nuage.

L'initiative de la Tunisie visant à réglementer la cybersécurité à travers le décret-loi n° 2023-17 du 11 mars 2023 relatif à la cybersécurité, accompagné des arrêtés de septembre 2023 réglementant ce nouveau cadre est une étape cruciale vers un avenir numérique sécurisé et prospère.

Ces réglementations mettent en évidence l'engagement de la Tunisie à faire face aux défis de la cybercriminalité, de la protection des données, et de la continuité des activités dans un monde de plus en plus connecté. Elles définissent des normes rigoureuses pour les prestataires de services informatiques en nuage, promouvant ainsi la confiance des utilisateurs et la croissance de l'économie numérique.

En anticipant les menaces émergentes et en exigeant la conformité aux normes internationales, la Tunisie renforce sa position en tant que leader régional en matière de cybersécurité. Ces mesures ne servent pas seulement à protéger les données gouvernementales et commerciales, mais aussi à encourager l'innovation et la transformation numérique au sein du pays.

L'avenir s'annonce prometteur, avec des opportunités nouvelles pour les entreprises locales et internationales de contribuer à la modernisation de l'infrastructure numérique tunisienne. La cybersécurité devient un pilier essentiel de la transformation numérique, permettant à la Tunisie de prospérer dans une économie mondiale de plus en plus axée sur la technologie.

Cependant, cette route vers la sécurité numérique ne sera pas sans obstacles. La collaboration continue entre le gouvernement, le secteur privé, la société civile et les acteurs internationaux sera cruciale pour relever les défis futurs et garantir une cybersécurité robuste et évolutive.

La Tunisie se positionne fermement sur la voie d'une société numérique sûre et novatrice