POLITIQUE D'ARCHIVAGE ELECTRONIQUE DE LA DIRECTION GENERALE DU TRESOR ET DE LA COMPTABILITE PUBLIQUE

Référence :
DGTCP-DDA-PS4-POL-462-2024
Version : 2
Date de rédaction : 27/05/2024

Objet : Le document présente la Politique d'Archivage Électronique du Trésor Public.

Rédaction du document	Vérification du document	Validation du document
Madame OURIGOU Biké Léonie épouse DJOLAUD *Sous-Directeur de la Numérisation* Visa :	**Madame LEGRE Evelyne épouse BERTE** *Directeur de la Documentation et des Archives* Visa :	**DIRECTION GENERALE DU TRESOR ET DE LA COMPTABILITE PUBLIQUE** Visa : MINISTERE DES FINANCES ET DU BUDGET – DIRECTION GENERALE DU TRESOR ET DE LA COMPTABILITE PUBLIQUE – RCI Pour le Directeur Général du Trésor et de la Comptabilité Publique et par Délégation Le Directeur Général Adjoint SANOGO BAFETEGUE
Gestionnaire du document	Direction de la Documentation et des Archives	
Destinataires pour action	**Destinataires pour information**	**Validité**
Tous les Services de la DGTCP	Tous les Services de la DGTCP	A compter du : 03 -12- 2024

SOMMAIRE

SIGLES ET ABREVIATIONS

DDA : Direction de la Documentation et des Archives

DGTCP : Direction Générale du Trésor et de la Comptabilité Publique

DMG : Direction des Moyens Généraux

DSI : Direction des Systèmes d'Information

DUA : Durée d'Utilité Administrative

PAE : Politique d'Archivage Électronique

PS4 : Processus Support N°4

RM : Records Management

SAE : Système d'Archivage Électronique

GLOSSAIRE

Archive électronique : Document sous forme numérique, quels que soient sa date et son support, produit ou reçu par tout service ou organisme public ou privé, dans l'exercice de ses activités.

Authentification : procédé visant à vérifier l'identification d'une personne physique par des moyens techniques, tels que mots ou phrases de passe, un code secret, une réponse à un défi ou encore une sécurisation numérique (Certificat).

Certificat : Document sous forme électronique attestant du lien entre l'identité du titulaire et les données de vérification de la signature électronique.

Communication : Fait de porter l'archive électronique ou toutes informations relatives à l'archive électronique, à la connaissance d'une personne déterminée ou d'un groupe d'intéressés.

Conservation : Opération juridique ou matérielle destinée à assurer la sauvegarde d'un droit, d'une chose, d'un patrimoine.

Consultation : Interrogation du système d'archivage électronique en vue d'en exploiter le contenu.

Contenu d'information : Ensemble d'informations constituant l'objet principal de la pérennisation.

Empreinte numérique : Ensemble de bits qui caractérise un document numérique. Toute modification du document numérique entraine une emprunte différente qui révèle la modification par comparaison avec la première emprunte.

Élimination (ou Destruction) : Opération qui consiste à détruire l'archive électronique après un visa d'élimination.

Journaux d'évènement : Enregistrement d'un ensemble de données relatives aux différentes opérations effectuées ou anomalies survenues au sein d'un système d'archivage électronique et destiné à assurer la traçabilité du service. Par ailleurs, ces journaux doivent être conservés pendant une période à définir et donc faire l'objet d'une procédure de sauvegarde particulière.

Métadonnées : Description de l'archive électronique. Les métadonnées portent à la fois sur le contenu, la gestion et le format.

Migration de formats : Opération qui consiste à migrer le contenu de certains types de supports vers d'autres types afin que le format de fichier utilisé pour la conservation des archives électroniques reste adapté compte tenu de l'évolution des technologies.

Migration de supports : Opération qui consiste à migrer le contenu de certains types de supports vers d'autres types afin d'anticiper l'obsolescence du support concerné.

Politique de sécurité : Ensemble de règles qui définissent les exigences physiques, techniques et logiques afin de garantir un niveau de sécurité déterminé.

Service producteur : Entité qui a initialement reçu ou produit les archives électroniques et qui en est propriétaire. Le service producteur et le service d'archives électroniques peuvent être assurés par une même personne juridique.

Service versant : Entité qui verse les archives électroniques à un service d'archives électroniques.

Support : Tout instrument permettant à l'utilisateur de stocker les informations de telle sorte que celles-ci puissent être consultées ultérieurement pendant une période adaptée à l'objectif de ces informations, et permettant la reproduction exacte des informations stockées.

Stockage : Opérations consistant à garder des archives électroniques sur un support pendant une durée déterminée et dans un format pérenne.

Système d'Archivage Électronique : Système consistant à recevoir, conserver, traiter, restituer des archives électroniques et qui s'appuie sur une plateforme informatique.

Utilisateur : Toute personne physique ou morale autorisée à utiliser un Système d'Archivage Électronique.

Versement : Transmission par un Service versant d'archives électroniques à un Service d'Archivage Électronique.

I. CONTEXTE

Une Politique d'Archivage Électronique se définit comme un document de référence qui précise les exigences juridiques, fonctionnels, opérationnels, techniques et de sécurité, qu'un Service d'Archives doit respecter, afin que l'archivage électronique mis en place puisse être conforme à la législation, la réglementation et aux normes en vigueur.

L'évolution institutionnelle et technologique de la Direction Générale du Trésor et de la Comptabilité Publique marquée, d'une part, par de nouvelles orientations stratégiques et la création de Services engendrant des besoins documentaires à satisfaire, ainsi que la modification de la cartographie de ses processus d'autre part, nécessite la mise à jour des outils de gestion.

Au regard de ce nouveau contexte, qui impacte l'ensemble des activités des Services, il apparait nécessaire de réviser la ligne conductrice de la gestion des archives électroniques dans les Services du Trésor Public.

De ce fait, la Politique d'Archivage Électronique, guide utile à la prise de décision, qui donne la position officielle du Trésor Public dans le domaine de la gestion des documents électroniques doit être adaptée à ces différents changements.

La Direction de la Documentation et des Archives (DDA), Pilote du Processus Support n° 4 (PS4) « Gérer le Système d'Information Documentaire » a l'obligation, conformément au décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique, et aux recommandations de la norme ISO 15489-1 :2016 (F) (Information et documentation - Gestion des documents d'activités. Partie 1 : Concepts et principes – Point 6 : Politiques et responsabilités) de proposer une Politique d'Archivage Électronique des documents.

La présente Politique d'Archivage Électronique fournit l'ensemble des spécifications relatives aux mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, l'archivage, la consultation, la sécurité et la communication des documents numériques du Trésor Public.

II. OBJET DE LA POLITIQUE D'ARCHIVAGE ELECTRONIQUE AU TRESOR PUBLIC

La présente Politique d'Archivage Électronique précise le cadre législatif, réglementaire et normatif qui encadre l'archivage électronique des documents au Trésor Public.
Elle définit les acteurs et leurs responsabilités sur le Système d'Archivage Électronique (SAE), formalise les engagements de services à respecter par les différents acteurs du processus d'archivage électronique.

III. CADRE LEGISLATIF, REGLEMENTAIRE ET NORMATIF

III.1. Cadre législatif

Il s'agit de :

- la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- la loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques en son chapitre 8 sur l'archivage des documents électroniques ;
- la loi n° 2013-867 du 23 décembre 2013 relative à l'accès à l'information d'intérêt public ;
- la loi n° 2023-892 du 23 novembre 2023 portant statut général de la Fonction Publique en son article 35 sur les obligations du fonctionnaire ;
- l'ordonnance n° 2016-660 du 20 septembre 2016 portant prévention et lutte contre la corruption et les infractions assimilées ;
- l'ordonnance n° 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

III.2. Cadre réglementaire

Il s'agit :

- du décret n° 76-314 du 4 juin 1974 portant règlement général des Archives Nationales ;
- du décret n° 2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;
- du décret n° 2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- du décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

- du décret n° 2021-914 du 22 décembre 2021 fixant les règles pour la conception, la réalisation et la gouvernance des projets publics d'infrastructures, d'équipement et de plateformes de services numériques ;
- du décret n° 2021-915 du 22 décembre 2021 portant adoption de la politique de sécurité des systèmes d'information de l'administration publique ;
- du décret n° 2021-916 du 22 décembre 2021 portant adoption du Référentiel Général de Sécurité des Systèmes d'Information et du plan de protection des infrastructures critiques ;
- du décret n° 2023-960 portant organisation du Ministère des Finances et du Budget ;
- de l'arrêté n° 511/MPTIC/CAB du 11 novembre 2014 portant définition du profil en fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel ;
- Arrêté n° 0246/MEF/DGTCP/DEMO du 17 mai 2023 portant organisation de la Direction de la Documentation et des Archives et fixant ses attributions ;
- Arrêté n° 0642/MFB/DGTCP/DSDI du 30 novembre 2023 portant organisation et attributions des Antennes Régionales de la Direction de la Documentation et des Archives (DDA) et fixant leur ressort territorial.
- de la décision n° 2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) en date du 16 mai 2019 portant Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) ;
- de la Politique d'Archivage de la Direction Générale du Trésor et de la Comptabilité Publique.

III.3. Cadre normatif

Il est relatif :

- à la norme NF Z 42-013 de mars 2009 sur les spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes (équivalant à la norme ISO 1441-1) ;
- à la norme ISO 15489-1 :2016 (F) (Information et documentation - Gestion des documents d'activités. Partie 1 : Concepts et principes – Point 6 : Politiques et responsabilités) ;

- à la norme ISO 19005-4 :2020 / Gestion des documents – Format de fichier de document électronique pour la conservation à long terme - Partie 4 : Utilisation de la norme ISO 32000-2 (PDF/A-4) ;
- à Dublin Core, recommandation pour la description bibliographique (métadonnées) des documents.

IV. ACTEURS ET RESPONSABILITES

IV.1. La Direction Générale

- valide la Politique d'Archivage Électronique et les procédures de gestion des archives électroniques ;
- garantit la disponibilité des moyens nécessaires à la gestion des archives électroniques ;
- assure l'interface avec les autres administrations dans le cadre de la mise en œuvre de la Politique d'archivage électronique.

IV.2. La Direction de la Documentation et des Archives

- élabore les politiques et procédures de gestion des archives électroniques conformément à la législation, la réglementation et aux normes ;
- procède au déploiement de la Politique d'Archivage Électronique par la sensibilisation et la formation des acteurs ;
- s'assure de l'appropriation par le personnel de la Politique d'Archivage Électronique et rend compte à la Direction Générale ;
- assiste le personnel à l'application de la Politique d'Archivage Électronique, aux procédures et aux principes de gestion des archives électroniques ;
- sensibilise le personnel à se conformer à la Politique d'Archivage Électronique ;
- suit et évalue la mise en œuvre de la Politique d'Archivage Électronique.

IV.3. La Direction des Systèmes d'Information

- Conseille la Direction de la Documentation et des Archives (DDA) pour l'acquisition de matériels informatiques concernant la gestion des documents électroniques ;
- assure la sauvegarde sécurisée des données numériques stockées dans les systèmes informatiques du Trésor Public ;

- assiste la Direction de la Documentation et des Archives (DDA) dans le développement et l'exploitation du système d'archivage électronique du Trésor Public.

IV.4. La Direction des Ressources Humaines

- détermine de concert avec la Direction de la Documentation et des Archives, le profil et le personnel nécessaire à la gestion du SAE ;
- met à disposition le personnel.

IV.5. La Direction des Moyens Généraux

La Direction des Moyens Généraux en relation avec la DDA et la DSI, assure la mise à disposition des équipements nécessaires.

IV.6. La Direction de la Formation

La Direction de la Formation (DF) réalise, en liaison avec la DDA des séances de renforcement des capacités du personnel en charge de la gestion des documents des Services du Trésor Public et des utilisateurs du SAE.

IV.7. Les Services du Trésor Public

- contribuent au déploiement de la Politique d'Archivage Électronique dans leurs services ;
- veillent au respect de la Politique d'Archivage Électronique dans leurs services ;
- s'assurent que leurs agents produisent et archivent les documents électroniques concernant toutes les actions qu'ils mènent conformément aux procédures, normes et réglementations en archivage électronique ;
- saisissent la Direction de la Documentation et des Archives (DDA) en cas de difficultés liées à l'application de la Politique d'Archivage Électronique.

IV.8. Les Administrateurs du Système d'Archivage Électronique

- exercent leurs activités dans le respect des textes législatifs, réglementaires et normatifs qui encadrent le domaine ;
- s'engagent à respecter les procédures et procédés déterminés dans la présente Politique d'Archivage Électronique pour mener leurs activités ;
- informent la DDA de toutes difficultés rencontrées dans l'exercice de leurs activités.

IV.9. Les utilisateurs

- doivent respecter les conditions de consultation et de communication afférentes au Service d'archivage électronique ;
- doivent également respecter la confidentialité des documents et ne pas tenter d'y accéder s'ils ne disposent pas de droits d'accès ;
- s'engagent, dans la mesure où ils disposent d'un code d'accès personnel (authentification par login, mot de passe, etc.), à les conserver confidentiel et à en faire un usage sous leurs contrôle exclusif.

V. ENGAGEMENTS DE SERVICE

V.1. Identification et authentification des archives

Tout document électronique produit est destiné à être archivé une fois sa fonction première remplie. Il est pour cela identifié pour en déterminer l'authenticité et les conditions de conservation optimales.

La Direction de la Documentation et des Archives :

- Identifie les documents électroniques pertinents et importants à archiver en fonction de critères définis ;
- Établit un inventaire détaillé avec métadonnées (date, source, etc.) ;
- Attribue les métadonnées pour faciliter la recherche ;
- Assure l'authentification des documents pour certifier leur origine et leur intégrité.

V.2. Pérennité des archives électroniques

La pérennité d'un document est sa capacité à être conservé et accessible dans le temps sans subir de dégradation ou de perte d'information.

Pour s'assurer de la pérennité des documents électroniques la DDA en liaison avec la DSI s'engage à :

- privilégier les formats ouverts et standardisés dont l'usage est largement adopté. Le choix d'un format très utilisé réduit les risques qu'il ne soit pas maintenu dans le temps. Les formats PDF/A pour les documents textuels et TIFF pour les images sont prescrit ;
- générer des métadonnées sur les documents pour permettre leur traçabilité ;

- mettre en place des méthodes pour contrôler l'intégrité du document afin de garantir qu'il n'a pas été altéré depuis sa création ;
- limiter l'accès des documents aux personnes autorisées ;
- éviter le piratage en sécurisant les serveurs où sont stockés les informations. Les données peuvent être cryptées pour garantir leur protection.

V.3. Disponibilité du SAE et des informations qu'il conserve

Il faut entendre par disponibilité le fait, pour les utilisateurs du SAE, de pouvoir accéder au moment voulu aux données et aux fonctionnalités du système.
Dans le cadre du SAE, l'engagement de service en matière de disponibilité est important et doit être respecté par la DSI.

V.4. Traçabilité des opérations (journaux)

L'ensemble des opérations effectuées au sein du SAE doit être enregistré et tracé au sein de journaux qui sont eux-mêmes archivés dans le système.
Afin de constituer un ensemble de données à la fois suffisantes et cohérentes en matière de traçabilité, deux (2) grands types d'évènements doivent être enregistrés par le SAE :

- les événements ayant trait à l'exploitation du système (logs de connexion, communications, etc.) dans le journal de l'application ;
- les événements qui affectent les archives elles-mêmes (contrôles au moment du versement, migration de format, modification de métadonnées, etc.) dans le journal du cycle de vie.

V.5. Intégrité des informations conservées par le SAE

L'intégrité est la caractéristique d'une information qui n'a subi aucune altération ou modification intentionnelle ou accidentelle.
Le SAE doit garantir l'intégrité de l'ensemble des informations qu'il conserve. Cette garantie repose sur un mécanisme de prise et de vérification d'empreintes numériques, régulières et systématiques.
Dans le cas où une alerte relative à la perte d'intégrité d'un document est émise par le système, la DDA doit informer immédiatement le Service producteur.

V.5.1. Intégrité des journaux

Les journaux doivent être conservés dans les mêmes conditions de sécurité et d'intégrité que les archives auxquelles ils se rapportent. Ils doivent être horodatés une fois par jour, y compris en cas d'absence d'activité, et la continuité de la journalisation doit être assurée par un mécanisme de chaînage des journaux.

V.5.2. Conservation des journaux

Le journal de l'application doit être conservé pendant toute la durée de vie du système.
Le journal du cycle de vie doit être conservé pendant toute la durée de vie des archives.
En cas de restitution des archives, le journal doit être restitué avec les archives auxquelles il se rapporte et est éliminé du système initial.

V.5.3. Consultation des journaux

Le journal de l'application doit être communiqué, à la demande des utilisateurs par la DDA et par extrait uniquement.
Le journal du cycle de vie des archives doit être disponible pour les utilisateurs dans le SAE.

V.6. Confidentialité des informations conservées dans le SAE

La DDA doit garantir la confidentialité des informations conservées dans le SAE du Trésor Public, c'est-à-dire que les informations ne sont disponibles et divulguées qu'aux personnes ou processus autorisés.
Un contrat de service doit définir la liste des utilisateurs du SAE habilités à consulter les archives versées.

V.7. Sécurité du SAE et contrôle des accès

V.7.1. Respect des bonnes pratiques en matière de sécurité

La mise en œuvre des mesures de sécurité et de contrôle des accès doit se faire dans le respect strict des éléments de sécurité prévus dans la Politique de Sécurité et supervisée par la Direction des Systèmes Informations (DSI).
L'architecture réseau des systèmes informatiques devant supporter les fonctions du SAE doit respecter les bonnes pratiques en matière de sécurité réseau (cloisonnement,

séparation des environnements (test/production), règles de filtrage, robustesse des équipements réseau).

V.7.2. Contrôle des accès au système et aux locaux de stockage

Le SAE doit être accessible, physiquement et logiquement, qu'à des personnes nominativement autorisées. Les restrictions d'accès aux systèmes et informations doivent être définies conformément à leurs besoins de sécurité et à la criticité des actions autorisées sur les données et ressources. Les utilisateurs du SAE doivent faire l'objet d'authentification par identification personnelle.

Les locaux abritant le SAE doivent faire l'objet de contrôles d'accès physique empêchant l'accès à des personnes non autorisées. Les locaux doivent être protégés contre les accidents et pannes dus à l'environnement (dégâts des eaux, incendies, pannes électriques, pannes de la climatisation, pannes des réseaux de télécommunication).

VI. REVISION ET VALIDATION DE LA POLITIQUE D'ARCHIVAGE ELECTRONIQUE

VI.1 Révision de la Politique d'Archivage Électronique

La Politique d'Archivage Électronique doit être tenue à jour en fonction de l'évolution institutionnelle et technologique de la Direction Générale du Trésor et de la Comptabilité Publique.

VI.2 Validation de la Politique d'Archivage Électronique

La Politique d'Archivage Électronique a été validée par la Direction Générale du Trésor et de la Comptabilité Publique.