GP57

n°57
129 euros avec guide n°58

archimag.com
[STRATÉGIES & RESSOURCES DE LA MÉMOIRE & DU SAVOIR]

guide pratique

une publication du groupe serda

sécurité de l'information et archivage électronique

GP57

préface

La stabilité est-elle synonyme de sécurité ? En tout cas, en matière de gestion de l'information, mieux vaut ne pas compter dessus !

Parce que l'information elle-même est mouvante. Les flux sont continus, le document est construit dynamiquement, à partir de multiples sources, et s'ajoutent des données générées en masse qu'il faut aussi prendre en compte dans le système d'information. À tel point que pour raisonner en cycle de vie de l'information, en document vital, en preuve, mieux vaut penser aussi métadonnées et journal transactionnel ou autres traces. Nous vivons bien désormais dans l'ère de la trace.

La première partie de ce guide pratique en montre plusieurs signes. La version 2016 de la norme Iso 15489-1 sur le records management en tient compte. S'agissant des archives, la loi du 8 juillet 2016 relative à la liberté de la création, à l'architecture et au patrimoine va dans le même sens. La blockchain, qui émerge avec de nouvelles offres, en a fait un principe de fonctionnement. Et si des failles de sécurité peuvent apparaître, profitant de cette mouvance, la lutte s'organise : lutte contre la fraude documentaire, techniques

Michel Remize

cryptographiques, encadrement de l'archivage dans le cloud.

Ce guide pratique livre aussi dans une deuxième partie toute une série de conseils pour sécuriser son système d'information ou faire nécessairement évoluer son système d'archivage électronique. Il s'agit aussi peu à peu pour les acteurs concernés de se mettre à l'archivage électronique public avec le programme Vitam. Quant aux données personnelles, elles réclament une vigilance toute particulière, avec parfois la nécessité de les anonymiser. Et vos bâtiments sont-ils eux aussi sécurisés ? La troisième partie s'intéresse aux outils et solutions : supports d'archivage, cas particulier de l'hébergement des données de santé, signature électronique, anonymisation, solutions de KYC (know your customers), matériels de destruction.

Des témoignages et retours d'expérience constituent la quatrième et dernière partie.

Mais ce guide *« sécurité de l'information et archivage électronique »* (numéro 57) a son complément : le guide *« durées de conservation et tableaux de gestion »* (numéro 58). Celui-ci débute par un important volet juridique (question de la prescription, données personnelles…). Les tableaux de gestion de douze domaines d'activité sont fournis. Il est réalisé en partenariat avec le cabinet d'avocats Alain Bensoussan Avocats Lexing.

Bonne lecture ! ■

Michel Remize
[Rédacteur en chef]

nous faisons Archimag

Serda édition-IDP
24, rue de Milan, F-75009 Paris
Tél. : +33 (0)1 55 31 92 30
Fax : +33 (0)1 44 53 45 01
infos@archimag.com
www.archimag.com

contacts e-mail
prenom.nom@archimag.com

rédaction
rédacteur en chef
Michel Remize
directrice de la rédaction
Louise Guerre
directeur de la publication
Pierre Fuzeau

l'équipe de rédacteurs
Clémence Jost, Éric Le Ven, Bruno Texier
ont collaboré à ce guide pratique
voir en page 3
site web, newsletter
Clémence Jost
conception graphique
Julio Arias-Arranz, Arncoat
maquette
Bruno Dalèle, Exeterra.fr

publicité
Cathy Potel
01 55 31 92 30
responsable marketing et commercial
Alexandre Corbier
01 44 53 45 00
vente au numéro
service abonnement
Suzanne Amia
suzanne.amia@archimag.com
réclamations, infos :
suzanne.amia@archimag.com
BP 95-92244 Malakoff Cedex
tarifs et conditions d'abonnement
valables jusqu'au 31-12-2017
France : 1 an, 125 euros
France : 2 ans, 228 euros
Tarif étudiant : 1 an, 30 euros
Tarif demandeur d'emploi : 1 an, 57 eurosTarif demandeur d'emploi : 1 an, 54 euros
Vente au numéro : 18 euros

imprimeur
Inore Groupe Impression
4 rue Thomas Edison
58640 Varennes Vauzelles
éditeur
IDP Sarl, au capital de 40 000 euros
Information, documentation, presse
N° de commission paritaire : 1221 T 85484
ISSN : 2260-1708
Dépôt légal à parution du numéro
crédits photos
Couverture : © Fotolia
Intérieures : droits réservés, sauf mentions différentes

annonceurs
Archimède : 2e de couverture, 51
IDP : 2, 17, 33, 47, 53, 55, 3e de couverture
Serda Formation : 4e de couverture
Archimag sur les réseaux sociaux
Facebook
→ www.facebook.com/pages/archIMAG/102327599812643
Twitter
→ twitter.com/ArchimagRedac

Archimag est une publication du groupe Serda.

Ce document est imprimé sur papier certifié PEFC

sommaire

[horizons]

[bonnes pratiques]

[solutions]

[retour d'expérience]

auteurs et experts

Polyanna Bigle
avocate au cabinet Alain Bensoussan

Caroline Buscal
manager Serda

Sylvie Dessolin
présidente pour l'AAF de la commission Afnor/CN46-11, senior consultant information and data governance, compliance, records management, Sopra Steria

Chloé Dornbierer
étudiante en master 2 Propriété intellectuelle et nouvelles technologies, Aix-Marseille Université

Éric Dupuis
RSSI, Orange Cyberdefense

Clémence Jost
journaliste webmaster Archimag

Arnaud Jules
directeur gestion et conservation de l'information, Orange

Dimitri Mouton
consultant et fondateur de Demaeter

Éric Le Ven
journaliste Archimag

Mélanie Rebours
directrice de la diffusion et des partenariats du programme Vitam

Michel Remize
rédacteur en chef Archimag

Guy Saignes
directeur technique Opus Conseils

Michel Thomas
consultant expert

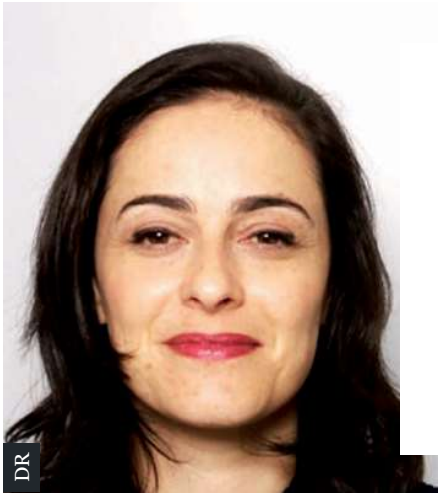
l'ère de la trace

Dans un monde surinformé et ultra connecté, le document semble perdre peu à peu sa place de référence. Ce qui compte pour l'entreprise n'est pas tant de conserver des documents, mais de disposer de traces et de preuves de traces. S'ouvre une nouvelle ère.

En 1956, IBM était parvenu à construire un disque dur d'une capacité de 5 mégaoctets. Près de soixante ans plus tard, en 2015, les 10 téraoctets étaient atteints par le fabricant HGST, filiale de Western Digital. Et devoir gérer des pétaoctets devient aujourd'hui courant. 10 puissance 6, 10 puissance 12, 10 puissance 15... Autant de zéros pour signifier la croissance exponentielle de l'information que nous créons.

différentes définitions ou notions juridiques

Mais paradoxalement, c'est au moment où nous produisons autant d'informations et en particulier de documents, en mettant en place quantités de lois et normes pour encadrer leur gestion et leur archivage (1), qu'est remis en cause le document tel qu'on l'entend - ou l'entendait. Professeur en sciences de l'information et de la communication, Jean-Michel Salaün rappelle : *« Pour la plupart des textes réglementaires ou des normes, le document est un objet (matériel ou électronique) sur lequel est consignée une information, en anglais on dira un record, un enregistrement »* (2). De fait, en droit français, reconnaît Polyanna Bigle, avocate au cabinet Alain Bensoussan, *« on se retrouve avec différentes définitions ou notions juridiques : écrit et écrit électronique, acte (authentique ou sous signature privée), support durable et support papier (Code de la consommation, par exemple), document administratif et document électronique du règlement eIDAS »*. Ce règlement européen du 23 juillet 2014 sur *« l'identification électronique et les services de confiance pour les transactions électroniques »* entend le document électronique comme *« tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel »* (3).


DR

« sur le plan juridique, la notion d'original ne disparaît pas »
Polyanna Bigle, avocate au cabinet Alain Bensoussan

le document très chahuté

Papier, électronique, dématérialisé : dans la réalité, le document est très chahuté. Les usages ont changé. On se moque du support devenu bien plus souvent électronique que papier. Celui-ci se révèle éphémère comme jamais. Combien de documents à peine imprimés, déjà jetés ?
Un document papier se scanne facilement, grâce non seulement à du matériel bureautique, mais aussi à un simple smartphone équipé d'une application. On commence à lire une information sur un support pour continuer sur un autre : nombreux sont ceux qui parcourent leurs mails sur leur mobile le matin dans les transports, attendent d'être au bureau pour lire leur sélection et traiter ce qui doit l'être. La mobilité fait de plus en plus d'adeptes.

des contenus malmenés ou surmenés

De plus, les contenus eux-mêmes sont malmenés ou surmenés. Combien de documents sont likés ou tweetés sans même avoir été lus ? Il ne s'agit pas que du grand public, même dans les entreprises, on encourage les réseaux sociaux et les like.
Le texte intégral permet d'aller à l'unité d'information, directement, l'extraire pour s'en servir, sans s'intéresser à la totalité du document.
Avec le travail collaboratif, servi par de plus en plus d'outils adaptés, les documents sont partagés et traversent de multiples étapes de création, d'enrichissement, de correction, d'édition ; ils n'ont pas forcément une validation finale et définitive.

20 conseils pour sécuriser son information

La sécurité informatique est devenue plus que jamais la priorité des organisations, et ce, quels que soient leur taille ou leur secteur d'activité tant les menaces de piratage, d'intrusion, de destruction des données, de blocage des serveurs se succèdent au fil des mois. C'est pourquoi il est important de prendre conscience du danger et suivre les vingt conseils suivants...

Le nombre d'incidents liés à la sécurité informatique aurait augmenté de 38 % entre 2015 et 2016 en Europe et, rien que pour la France, 24 000 attaques auraient été déjouées en 2016 (*source Ministère de la France*). Avec la mobilité, l'IoT et la circulation croissante des données, les choses ne sont pas près de s'arranger. Malgré les faits, nombre d'entreprises françaises et européennes continuent à sous-estimer l'impact des cyberintrusions, faute de compétences en interne. D'où une série de mesures proposées par la Commission européenne pour faire en sorte que d'ici 2020, l'Europe soit mieux armée pour contrer les cyberattaques. 1,8 milliard d'euros seront d'ailleurs investis pour cela.

le facteur humain

Si des outils pour sécuriser l'information existent bel et bien, le facteur humain reste le principal vecteur de fuites et d'attaques. Tout l'or du monde ne sera d'aucun effet si les hommes ne sont pas d'abord sensibilisés et formés à cette urgence sécuritaire.

1. prendre la menace au sérieux

Beaucoup considèrent, à tort, que les PME ne sont pas des cibles d'attaque intéressantes. Les faits disent pourtant le contraire. Toutes les organisations constituent des cibles potentielles. Aucune ne fait exception. Qu'il s'agisse de ransomwares, de logiciels de phishing, de malwares ou de déni de service (DDoS), les attaques informatiques ciblent tout le monde : particuliers, petites entreprises et grands groupes. Si elle est réussie, une attaque peut être particulièrement onéreuse et sérieusement nuire à la réputation de la marque.

2. éduquer les utilisateurs

Le comportement des utilisateurs constituant la plus grande vulnérabilité d'une entreprise, une bonne sécurité repose donc sur l'éducation et le suivi des utilisateurs. Au fond, peu importe la qualité des équipes de sécurité et l'efficacité de la technologie : la sécurité restera faible si les professionnels de la sécurité ne parviennent pas à influencer les utilisateurs pour qu'ils respectent les principes de base en la matière. La sensibilisation à la sécurité de l'information devrait d'ailleurs être obligatoire au moment du recrutement. Les organisations devraient travailler à construire une culture de la sécurité, en adaptant le message aux fonctions et âges des utilisateurs.

3. sécuriser tous les vecteurs de menace

Les attaques modernes exploitent plusieurs vecteurs, notamment le comportement des utilisateurs, mais aussi les applications et les systèmes. Les principaux vecteurs d'attaque étant les e-mails, les applications web et l'accès à distance. Une sécurité complète doit englober tous ces vecteurs. Moralité : un simple pare-feu ne suffit plus. Il convient donc de multiplier les couches de sécurité. Autrement dit, de ne plus mettre tous ses oeufs dans le même panier et de ne pas faire confiance à un seul fournisseur (hardware ou software) pour protéger son réseau et ses applications. Ce qui revient à empiler les couches de sécurité de plusieurs fabricants ou éditeurs.

4. sécuriser les postes de travail

Les postes de travail doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une certaine période d'inactivité (10 minutes maximum). Les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau, à éteindre leurs postes lorsqu'ils quittent l'entreprise et à bien séparer les usages personnels des usages professionnels. Le contrôle de l'usage des ports USB sur les postes *« sensibles »* (interdisant par exemple la copie de l'ensemble des données contenues dans un fichier) est également fortement recommandé.

5. mettre en place une authentification multifactorielle

Ce type d'authentification (login et mot de passe et code à usage unique, code

records manager : le chef d'orchestre du bal des archives

Préoccupation de conservation des documents, aspects réglementaires, risques, sécurité, sensibilisation des collaborateurs, contexte à la fois numérique et papier… : le records management est apte à répondre à des problématiques complexes dans les organisations. Quatre records managers témoignent.

La volumétrie croissante des documents électroniques et papier au sein des organisations impose plus que jamais la mise en place d'un système d'archivage fiable. D'ordre essentiellement logistique à l'origine, cette nécessité est aussi devenue légale et réglementaire. D'autant que la maîtrise du patrimoine informationnel de l'organisation est un enjeu d'efficacité et de qualité. Le *« records manager »* est ainsi devenu le garant de cette politique. Issu de la documentation et des archives, il a l'aval de la direction générale et joue un rôle d'évangélisation auprès des producteurs de documents et des utilisateurs des systèmes d'archivage. Car l'enjeu est dorénavant moins technique que managérial et culturel. Il doit mettre en exergue la valeur stratégique de l'archive et instaurer la politique adéquate.

Yves Sarazin, PSA : les documents engageants sous contrôle

« Je suis à la croisée des chemins », explique Yves Sarazin, qui exerce au sein de la direction sureté groupe et est aussi rattaché au secrétariat juridique. Sa fonction au sein de PSA Peugeot Citroën couvre, en effet, plusieurs aspects. Il y a d'abord la fonction classique de conservation des documents en fonction de leur typologie. *« J'établis un référentiel de conservation et j'organise les documents engageants,* précise-t-il. *En fonction de la réglementation et des risques »*. Pour ce travail, il s'appuie essentiellement sur une équipe de juristes en interne. Mais sa mission va plus loin, puisqu'il veille à ce que les collaborateurs en charge des documents puissent appliquer ces règles. Ce, aussi bien pour les documents papier que pour les documents numériques. Enfin, il analyse les nouveaux besoins des différentes équipes et définit les règles de conservation pour les documents métier qui en seraient dépourvus. *« Nous définissons aussi les critères métier qui vont permettre de retrouver le document »*, confie-t-il.

maîtrise et gouvernance de l'information

En 2010 lorsqu'il a été nommé à ce poste, on ne parlait pas encore beaucoup de records management. La fonction est relativement nouvelle et va de pair avec l'essor des projets digitaux (notamment la dématérialisation de la relation client) et la volonté d'archiver les documents électroniques dès leur production. *« Ma mission est donc d'aller au contact des métiers pour connaître leurs besoins, voir ce qui doit être archivé ou gérer autrement »*, indique le responsable. En cas de document papier, il définit la meilleure approche pour pouvoir les archiver, élabore un plan de classement et s'occupe de la sécurité d'accès. *« Nous faisons du sur-mesure pour les besoins de chaque métier,* ajoute-t-il. *C'est une fonction d'autant plus riche qu'elle me permet également d'intervenir sur la problématique liée à la numérisation des documents papier »*.

Michel Cottin, RATP : gestionnaire du cycle de vie et de la conformité

Michel Cottin, lui, évolue dans un autre univers, mais son rôle n'est pas tellement différent. Tout nouveau à la RATP, il est l'héritier d'une longue tradition de service d'archives d'entreprise depuis les années 90. *« Nous faisons du records management et de la gestion du cycle de vie,* précise l'intéressé. *Nous sommes aujourd'hui en train d'élaborer un projet de tableau de gestion. Placée sous le régime des archives publiques, la RATP a, en effet, besoin de bien fixer les règles de conservation des archives »*. C'est une question de conformité.

à chaque ligne ses archives !

À la RATP, chaque ligne possède ses propres archives : pilotage et RH, gestion de l'infrastructure (tunnel, gare, accès, etc.), circulation des trains et des bus (ordres de marche) et sécurité (documents relatifs aux incidents, à la signalisation, etc.). *« Nous souhaitons sécuriser toutes ces archives,* renchérit Michel Cottin. *Avec une attention toute particulière pour celles qui décrivent la sécurité »*. Tel est le rôle du records manager. Suite à un déménagement, la RATP a également lancé un projet de gestion des archives pour la ligne 9. L'objectif étant de réduire leur volume et de mieux les organiser.

Informations relatives au paiement	Type de paiement utilisé Montant Numéro de référence du moyen de paiement Date et heure de la transaction	-	judiciaire	utile	papier/ électronique	1 an	destruction	La DUA s'applique à compter du jour de la création du contenu.	Art. 6, II LCEN 21 juin 2004 ; Décret d'application n° 2011-219 du 25 février 2011

11. Ressources humaines

11.1. Dossier individuel

Dossier	Typologie documentaire	Activité métier	Valeurs	Statut	Support de conservation recommandé	Durée de conservation (DUA)	Sort final	Observations	Texte réglementaire de référence
Dossier individuel de recrutement	Lettre de candidature et CV Lettre de recommandation Questionnaires/tests précédant l'embauche et leurs conclusions Lettre d'embauche Contrat de travail Attestation de prise de connaissance du règlement intérieur Extrait casier judiciaire Avenants au contrat de travail : promotion, mutations fonctionnelles ou géographiques, modification du temps de travail Convention de stage	suivi de dossier et contractuel	administra-tive/judiciaire	important	papier/ électronique	80 ans dans le secteur public / 10 ans dans le secteur privé	tri	Dans le secteur public, la DUA de 80 ans s'applique à compter de la date de naissance de l'agent : se référer à l'Art. 2 de l'arrêté du 21/12/2012. Dans le secteur privé, la DUA de 10 ans s'applique à partir de la date de sortie définitive du salarié de l'entreprise. Dans la cas du secteur public, les documents devant être absolument conservés 80 ans sont: - Tous ceux susceptibles d'avoir une influence sur les droits à la retraite (congés annuels non rémunérés, congés de longue durée ou d'invalidité...) - Le dossier de carrière - Le dossier médical Le reste peut être éliminé 5 ans après le départ définitif du salarié. Le tri est, dans ce cas, une pratique fréquente des organisations qui effectuent un échantillonnage de leurs dossiers et les conservent pour des raisons historiques.	Art. L3243-4 C. travail
Dossier carrière	Demande de détachement, de changement d'affectation Justificatifs des formations Justificatifs de qualifications pour le poste de travail occupé (diplômes...) Bilan de compétences Congé de validation des acquis de l'expérience Formation non spécifique Compte rendu d'entretien d'évaluation	suivi de dossier et contractuel	administra-tive/judiciaire	important	papier/ électronique	80 ans dans le secteur public / 10 ans dans le secteur privé	tri	Dans le secteur public, la DUA de 80 ans s'applique à compter de la date de naissance de l'agent : se référer à l'Art. 2 de l'arrêté du 21/12/2012. Dans le secteur privé, la DUA de 10 ans s'applique à partir de la date de sortie définitive du salarié de l'entreprise. Dans la cas du secteur public, les documents devant être absolument conservés 80 ans sont: - Tous ceux susceptibles d'avoir une influence sur les droits à la retraite (congés annuels non rémunérés, congés de longue durée ou d'invalidité...) - Le dossier de carrière - Le dossier médical Le reste peut être éliminé 5 ans après le départ définitif du salarié. Le tri est, dans ce cas, une pratique fréquente des organisations qui effectuent un échantillonnage de leurs dossiers et les conservent pour des raisons historiques.	Art. L3243-4 C. travail
Dossier de congés et absences	Demandes et documents de congés (parental, maladie, année sabbatique...) Arrêt maladie	suivi de dossier et contractuel	administra-tive/judiciaire	important	papier/ électronique	80 ans dans le secteur public / 10 ans dans le secteur privé	tri	Dans le secteur public, la DUA de 80 ans s'applique à compter de la date de naissance de l'agent : se référer à l'Art. 2 de l'arrêté du 21/12/2012. Dans le secteur privé, la DUA de 10 ans s'applique à partir de la date de sortie définitive du salarié de l'entreprise. Dans la cas du secteur public, les documents devant être absolument conservés 80 ans sont: - Tous ceux susceptibles d'avoir une influence sur les droits à la retraite (congés annuels non rémunérés, congés de longue durée ou d'invalidité...) - Le dossier de carrière - Le dossier médical Le reste peut être éliminé 5 ans après le départ définitif du salarié. Le tri est, dans ce cas, une pratique fréquente des organisations qui effectuent un échantillonnage de leurs dossiers et les conservent pour des raisons historiques.	Art. L3243-4 C. travail