2019

White paper series
Édition 6

– CLASSIFICATION –
DES DONNÉES

OEA | Plus de droits pour plus de personnes

aws

— CLASSIFICATION —
DES DONNÉES

CRÉDITS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Equipo técnico OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Kadri Kaska
Elsa Neeme
Klaid Mägi
Lauri Luht

Equipo técnico AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTENU

— CLASSIFICATION —
DES DONNÉES

Introduction

1

Les organisations, les personnes et les milliards d'appareils connectés produisent, traitent et consomment toutes sortes de données par jour. Plus de 2,5 quintillions d'octets de toutes sortes de nouvelles données[1] sont produits, chaque jour, pour être analysés, traités et stockés. L'éventail des données est également varié, allant des uns et zéros provenant de simples dispositifs IdO (Internet des Objets) qui renseignent sur un événement on/off (par exemple, un détecteur de mouvement), les conditions météorologiques, le trafic, les transactions financières, la santé et aux médias sociaux, entre autres. De même, les gouvernements, qui font l'objet du présent document, produisent, gèrent et stockent des pétaoctets de données. La diversité des données nous amène à nous demander quelles sont les bonnes politiques qu'un gouvernement devrait suivre pour classifier et stocker les données qu'il détient. Les gouvernements ont répondu à cette question en élaborant des politiques de classification des données sous forme de lignes directrices précises, à l'intention des organismes gouvernementaux, décrivant la façon dont les différents types de données devraient être classés, protégés, manipulés, stockés et traités en fonction de leur niveau.

La première question souvent posée est la suivante : « Pourquoi ne pas simplement protéger toutes les données au plus haut niveau et gagner du temps ? » Pour les gouvernements, cela n'est tout simplement pas faisable sur le plan financier et annule certains autres avantages d'une classification et d'un étiquetage appropriés des différents types de données. Premièrement, les niveaux les plus élevés de protection des données impliquent des coûts supplémentaires. Il s'agirait donc de dépenser plus que ce qu'elles valent en termes de protection des données. D'un autre côté, si toutes les données sont traitées de la même façon et ne sont pas différenciées, il peut être difficile de mettre en œuvre des contrôles d'accès appropriés et les données sensibles peuvent être accessibles aux personnes qui n'ont pas de raison officielle d'avoir accès à ces données. Finalement, il est possible de réaliser des gains d'efficacité dans la gestion et la communication de données correctement organisées, regroupées, sécurisées et étiquetées en fonction de leur classification.

La classification des données permet aux organisations de réfléchir à leur sensibilité et leur impact commercial, ce qui les aide ensuite à évaluer les risques associés aux différents types

1 Forbes : Combien de données créons-nous chaque jour ? The Mind-Blowing Stats Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#49f394760ba9

de données. Des organismes de normalisation réputés, comme l'Organisation internationale de normalisation (ISO) et l'Institut national des standards et de la technologie (NIST, National Institute of Standards and Technology), recommandent des systèmes de classification des données pour que l'information puisse être gérée et sécurisée plus efficacement en fonction du risque relatif et de la criticité qu'elle représente, puis déconseille les pratiques qui traitent toutes les données de façon égale. Malgré le fait que chaque organisation traite et classifie les données en fonction de leurs besoins, de leurs règlements et même de leurs capacités respectives, il est toujours nécessaire d'établir un ensemble de contrôles de sécurité de base qui offrent une protection appropriée contre les vulnérabilités, les menaces et les risques proportionnellement au niveau de protection défini, notamment dans le secteur public.

Les avantages d'une classification efficace des données pour une organisation sont multiples. En effet, l'organisation est ainsi en mesure d'améliorer son accessibilité au données et son efficacité organisationnelle. Une classification efficace des données permet de s'assurer que l'information bénéficie d'une protection appropriée en fonction de sa sensibilité, de sa valeur et de sa criticité, ainsi que de la nature et du degré de risques liés à sa divulgation, détérioration ou destruction injustifiée.

Le but de ce livre blanc est de fournir des orientations pour l'élaboration d'un système de classification des données afin d'assurer la protection et l'accès à l'information produite et traitée par les gouvernements. Il convient de souligner qu'une politique de classification des données est nécessaire quel que soit le type d'infrastructure utilisé par une organisation : sur site, sur le cloud ou mobile. Une politique de classification des données fournit des directrices aux organisations quant au niveau de sécurité et aux processus associés au stockage et à la gestion des différents types de données. Les recommandations contenues dans ce livre blanc peuvent être appliquées quel que soit le type d'organisation. Néanmoins, elles visent principalement à présenter aux entités gouvernementales qui fournissent des services publics, des considérations clés à prendre en compte lors de ce processus.

|Structure|

Le présent Livre blanc vise à fournir des orientations pour l'élaboration d'un système de classification des données qui permette d'assurer la protection et l'accès à l'information produite et traitée par les gouvernements. Il évalue les approches de classification des données existantes tant au niveau national qu'international, afin de proposer un outil fonctionnel de classification des données et le moyen d'éviter tout risque potentiel de sousclassification ou surclassification des informations.

Ce Livre blanc est divisé en quatre sections : i. Principes de classification des données et de l'information ; ii. Quels sont les modèles existants du secteur public ? iii. Recommandations pour l'établissement d'un système de classification des données ; iv. Ressources recommandées permettant un aperçu des principes de la classification des données, ainsi que quelques recommandations pour leur mise en œuvre. Afin d'illustrer certains des modèles existants du secteur public, la section II présente une analyse de l'expérience des États-Unis, du Royaume-Uni et de l'Argentine en matière de mise en œuvre et de réglementation générale de la classification des données. Les études de cas des États-Unis et du Royaume-Uni sont particulièrement pertinentes étant donné leur niveau de rigueur et de sophistication. Le cas de l'Argentine présente, quant à lui, l'expérience d'un pays de la région de l'Amérique latine et des Caraïbes. Les recommandations de ce livre blanc doivent, avant tout, être appliquées au contexte et aux besoins de votre organisation dans l'établissement d'une stratégie de protection des données.

Principes de classification des données et de l'information

2

La mise en place d'une gestion de l'information, de façon générale, et de la classification des données, en particulier, peut varier selon le type d'organisation. Toutefois, certains principes fondamentaux sont communs à tous les gouvernements, organisations non gouvernementales et organisations commerciales. Les considérations qui suivent exposent six principes provenant de sources juridiques nationales (et régionales) ainsi que les instruments à disposition des organisations internationales en matière de gestion de l'information. Ces principes doivent être utilisés comme guide plutôt que comme point de référence unique et permanent dans l'élaboration ou l'amélioration d'une stratégie de gestion de l'information et de classification des données.

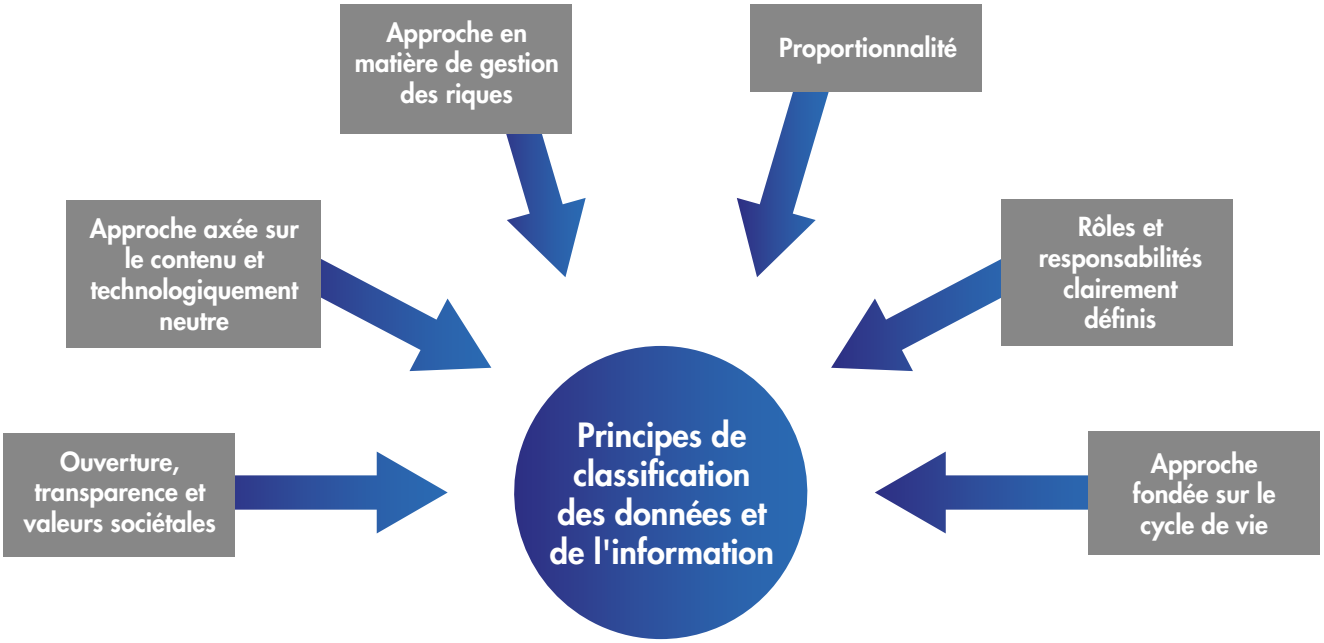

Figura 1- Principes de classification des données et de l'information

1. **Ouverture, transparence et valeurs sociétales :** La classification doit être utilisée avec prudence et conformément à la sensibilité, à la valeur et à la criticité des données. Les restrictions d'accès ne doivent être effectuées que dans les cas où la divulgation d'informations pourrait nuire aux intérêts légitimes et aux obligations légales de l'organisation elle-même, de son personnel ou de tiers. Dans de tels cas, les procédures spécifiées doivent être strictement observées de manière à s'assurer que l'information n'ait pas été divulguée délibérément ou par inadvertance. Le défi consistera à ne pas surclasser l'information pour des raisons de commodité ou praticité, au détriment de la transparence et de la confiance du public et ainsi priver les parties prenantes d'être maîtres de leurs propres décisions en matière de gestion des risques.

2. **Approche axée sur le contenu et technologiquement neutre :** Les informations doivent être classées en fonction de leur contenu et des risques associés à la diffusion de leur contenu, quels que soient leur format, support ou origine. Aucune discrimination fondée sur le format ou le support de l'information (analogique (papier) ou numérique) ne devra avoir lieu, qu'elle soit stockée dans un système d'information, sur des supports de stockage, sur des appareils mobiles ou sur le Cloud. De même, la décision de classification de l'information devra dépendre du contenu lui-même et ne devra pas nécessairement découler de la source sur laquelle elle se fonde, à laquelle elle répond ou à laquelle elle fait référence. Ainsi, le fait de se fier à des sources publiques ne devra pas automatiquement amener à ce que l'information agrégée puisse être rendue publique.

3. **Approche en matière de gestion des risques :** L'information devra être protégée en fonction de son degré de sensibilité, de sa valeur et de sa criticité. L'approche habituellement utilisée est graduelle et proportionnelle à la valeur et au risque. Un niveau de protection comprend l'ensemble des mesures visant à réduire les risques à un niveau acceptable, c'est-à-dire la gravité potentielle et la probabilité de divulgation de l'information. Pour déterminer le niveau de sensibilité et la valeur de l'information, il faut tenir compte à la fois du degré de dommage potentiel dans le cas de divulgation (divulgation non autorisée, modification ou perte) ainsi que de la valeur potentielle des données.

4. **Proportionnalité:** Les informations doivent être classées à un niveau approprié qui doit être aussi bas que possible, mais aussi important que nécessaire.

5. **Rôles et responsabilités clairement définis :** La politique et les processus devront être élaborés pour permettre la sécurité de l'information au sein de l'organisation et être ratifiés par l'engagement de la direction envers la sécurité de l'information.

6. **Approche fondée sur le cycle de vie :** Dans le cadre d'un système de gestion de l'information, le système de classification devra tenir compte de l'information tout au long de son cycle de vie : depuis sa création ou sa réception à sa destruction, en passant par son stockage, récupération, modification, transfert, copie et transmission. De plus, la politique de gestion de l'information et de traitement des données d'une organisation ne devra pas être gravée dans le marbre, mais pourra évoluer régulièrement afin de répondre aux besoins et aux attentes de l'organisation.

Quels sont les modèles existants du secteur public ?

3

La mondialisation a entraîné une tendance à la convergence de la terminologie de la classification des données. Cette convergence s'explique notamment par la rigueur des normes de l'industrie des technologies de l'information et de la communication (l'adhésion aux définitions ISO/CEI et NIST), les développements politiques et juridiques régionaux qui en résultent (en particulier dans l'Union européenne et ses États membres), mais tout particulièrement par les interactions et interdépendances entre domaines (la prise en compte croissante des réglementations sur la cybersécurité et la protection des données). Il est donc recommandé de tenir compte de ces bonnes pratiques lors de l'élaboration des définitions nationales.

Les États-Unis, le Royaume-Uni et l'Argentine ont établi des systèmes de classification des données du secteur public. Les gouvernements des États-Unis et du Royaume-Uni utilisent, tous deux, un système de classification à trois niveaux, la majorité des données du secteur public étant classée dans les deux niveaux inférieurs. Le cas de l'Argentine a été inclus comme exemple régional permettant d'observer la mise en œuvre et les difficultés rencontrées. La ville de Washington, D.C., pourrait également être prise comme modèle car largement applaudie pour la convergence de ses données ouvertes avec la classification de celles-ci et sans la composante de sécurité nationale. Les systèmes de classification des données comportent une courte liste des particularités et mesures ou critères connexes visant à aider les organisations à déterminer le niveau de classification approprié.[2]

|Les États-Unis d'Amérique|

Le gouvernement des États-Unis utilise un système de classification à trois niveaux mis à jour par le décret-loi 135261 et fondé sur l'impact potentiel sur la sécurité nationale en cas de divulgation (confidentialité) :

1.Confidentiel — Information dont la divulgation non autorisée risquerait vraisemblablement de porter atteinte à la sécurité nationale.

2.Secret— Information dont la divulgation non autorisée risquerait vraisemblablement de porter gravement atteinte à la sécurité nationale.

3.Top secret — Information dont la divulgation non autorisée risquerait vraisemblablement de causer des dommages exceptionnellement graves à la sécurité nationale.

2 Classification des données de AWS - Adoption du cloud sécurisé (juin 2018)

De plus, bien qu'il ne s'agisse pas d'une classification réelle, les États-Unis utilisent également l'expression « données non classifiées » pour désigner toute donnée qui ne soit pas classée selon les trois niveaux de classification officiels. Même dans le cas de données non classifiées, certaines réserves existent concernant les informations sensibles, telles que « Exclusivement réservé à l'usage officiel » (FOUO) ou « Informations non classifiées contrôlées » (CUI) qui restreignent la divulgation au public ou au personnel non autorisé. Cette classification ne tient pas compte des diverses lois en matière de protection des données fondées sur des types de données plus restreints comme le sont les données fiscales des particuliers, les données criminelles, les données relatives aux cartes de crédit, les données relatives aux soins de santé et autres.

En raison de l'étroitesse du système de classification américain, qui ne tient pas directement compte de l'intégrité et de la disponibilité des données dans ses niveaux de classification (facteurs qui devraient être requis pour évaluer les exigences en matière de protection de l'information), le NIST a élaboré un système de classification à trois niveaux fondé sur l'impact potentiel sur la confidentialité, l'intégrité et la disponibilité des informations et systèmes d'information applicables à la mission d'une organisation. La plupart des données traitées et stockées par les organisations du secteur public peuvent être classées comme suit:

- **Faible** — Effets négatifs limités sur les activités, les biens ou les personnes de l'organisation.

- **Modéré** — Effets négatifs indésirables sur les activités, les biens ou les personnes de l'organisation.

- **Élevé** — Effets négatifs graves sur les activités, les biens ou les personnes de l'organisation.

Classification des données	Niveau de sécurité du système
Non classifié	Faible à élevé
Confidentiel	Modéré à élevé
Secret	Modéré à élevé
Top secret	Élevé

Tableau 1 — Classification des données par rapport au niveau de sécurité du système

Pour de nombreuses autres administrations nationales, provinciales, étatiques et locales, ce double système de classification et de niveaux peut s'avérer trop complexe et inutile pour répondre aux besoins de sûreté de l'information. Dans ces cas-là, une option plus simple consiste à fusionner les deux concepts sous un seul terme « classification » qui aborderait tant la sécurité nationale (le cas échéant) que les trois piliers de la sûreté de l'information (confidentialité, intégrité et disponibilité) pour la mission et les activités d'une organisation. De ce fait, dans ce document, le mot « classification » fait référence à un classement plus globale en matière de confidentialité, intégrité et disponibilité plutôt qu'à la seule incidence sur la sécurité nationale.

|Royaume-Uni|

Le gouvernement du Royaume-Uni a récemment simplifié son système de classification en passant de six niveaux aux trois suivants:

1.Officiel — Activités et services commerciaux courants dont certains pourraient présenter des conséquences dommageables en cas de perte, vol ou publication dans les médias, mais dont aucun ne fait l'objet d'un profil de menace accru.

2.Secret—Informations très sensibles qui justifient de l'adoption de mesures accrues de protection contre des acteurs déterminés et hautement compétents (une divulgation pourrait nuire considérablement aux capacités militaires, aux relations internationales ou aux enquêtes contre la criminalité organisée grave).

3.Top secret — Les Informations les plus sensibles nécessitant des niveaux de protection les plus élevés contre les menaces les plus graves (une divulgation de ces informations pourrait causer la perte de nombreuses vies ou menacer la sécurité ou le bien-être économique du pays ou des pays amis).

90 % des données du gouvernement du Royaume-Uni ont traditionnellement été classées dans la catégorie « officiel »[3]. Le pays utilise un système d'accréditation flexible et décentralisée selon lequel les agences déterminent les fournisseurs de services cloud qui conviennent aux données « officielles » en se fondant sur les garanties de sécurité fournies par ceux-ci suivant 14 principes de sécurité sur le cloud[4]. La plupart des agences gouvernementales britanniques jugent approprié d'utiliser des fournisseurs de services cloud à grande échelle et réputés lorsqu'elles ont à travailler avec des données « officielles ».

Le gouvernement du Royaume-Uni a énoncé diverses considérations relatives à la sécurité de l'information stockée sur le Cloud :

1.Officiel — Les différents services de GCloud[5] conviennent à toutes les informations et tous les biens classés dans la catégorie Officiel. Néanmoins, il est exigé que tous les propriétaires de risques puissent comprendre, de façon complète, l'accréditation GCloud. Tous les services des technologies de l'information et de la communication (TIC) doivent continuer à suivre le processus de gestion des risques tel que défini dans les normes de sûreté de l'information du gouvernement britannique, en plus des approches architecturales standard qui doivent être hébergées au Royaume-Uni.

2.Secret— Tous les services des technologies de l'information et de la communication qui traitent ou stockent des informations secrètes doivent être accrédités, le cas échéant, conformément au modèle de menace secrète. L'Autorité technique nationale pour la sûreté de l'information (CESG) devra fournir Les modèles de conception spécifiques ou les conseils à mettre en œuvre. D'après une évaluation préliminaire des risques et conséquences de la mise en place de la fonctionnalité d'échange d'information hors du niveau secret, cette possibilité sera fortement limitée et gérée au moyen d'une accréditation spécifique de partage.

3.Top secret— Les systèmes des technologies de l'information et de la communication conçus devront bénéficier des accréditations nécessaires pour ne pas laisser filtrer le matériel top secret. Des conseils personnalisés en architecture peuvent s'avérer nécessaires.

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf

4 https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

5 Le cadre G-Cloud est un accord passé entre le gouvernement britannique et les fournisseurs de services cloud.

|Argentine|

Dès 2004, le gouvernement argentin a commencé à définir les conditions nécessaires à l'élaboration et à la mise en œuvre d'une stratégie nationale de protection des données. Cette stratégie initiale comprenait la création d'un modèle de politique de sécurité, la formation d'un comité de sécurité de l'information, l'établissement de ses fonctions ainsi que la nomination d'un coordinateur pour superviser le travail du comité. La politique a été formalisée en 2005 lorsque l'Office national des technologies (ONTI), l'entité argentine responsable de la transformation et de la mise en œuvre des solutions technologiques dans le secteur public, a promulgué le modèle de politique de sécurité de l'information, Décret N° 378, qui par la suite a été mis à jour et modifié en 2014, sur la base d'une série de recommandations issues de sa révision en 2013 puis connue sous le nom de Disposición 1/2015[i].

Dans le cadre de sa gestion des risques, cette politique définit les meilleures pratiques en matière de protection et de gestion des actifs. Les propriétaires des données et de l'information sont responsables de leur classification en fonction de leur degré de sensibilité puis doivent documenter et mettre à jour la classification de l'information et définir quels utilisateurs devraient avoir accès à l'information en fonction de leurs positions et rôles. Au sein de la classification, la politique devra être fondée sur les trois facteurs suivants : confidentialité, intégrité et disponibilité. Chacun des trois facteurs se place sur une échelle de 0 à 3 qui détermine ensuite le degré de protection à adopter. L'échelle est la suivante:

- **Faible criticité:** Les informations sont classées comme publique. Elles sont généralement connues et utilisées par toutes les personnes ou employés. Leur modification non autorisée peut être facilement réparée et ne compromet pas les activités de l'organisation.

- **Criticité moyenne:** Les informations sont classées comme réservées ou à usage interne. Elles peuvent être connues ou utilisées par certains employés de l'organisation et certaines autorités déléguées externes. Leur utilisation peut entraîner de légers risques ou pertes pour l'Agence, le secteur public national ou des tiers. Leur modification non autorisée peut être réparée, bien qu'elle puisse entraîner de légères pertes pour l'organisme public ou des tiers associés. Leur perte permanente ou d'une journée pourrait causer des dommages importants aux activités de l'organisation.

- **Criticité élevée:** Les informations sont classées comme confidentielles ou secrètes. Ces informations ne peuvent être connues que d'un groupe restreint d'employés, habituellement la haute direction de l'organisation, et leur divulgation ou utilisation non autorisée pourrait entraîner des pertes importantes pour le secteur public ou des tiers associés. Leur perte permanente pourrait causer de sérieux dommages à l'organisation.

i http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Recommandations pour l'établissement d'un système de classification des données

4

Les systèmes de classification des données existants reconnaissent différents niveaux de sensibilité, de valeur et de criticité de l'information, ainsi que divers niveaux de gravité et de probabilité de divulgation. À moins que les niveaux de sécurité de certaines données ne soient prescrits par la loi (tel est le cas des renseignements relatifs à la sécurité nationale ou à la protection de la vie privée) ou qu'ils ne nécessitent pas d'alignement sur des engagements régionaux ou internationaux, la définition des niveaux de sécurité sera laissée à la discrétion de chaque organisation. Cela ne signifie pas nécessairement que le respect des exigences légales nécessite d'une myriade de niveaux distincts. Lorsque le risque et les protections requises sont équivalents, il est possible d'organiser celles-ci sous un seul niveau de classification.

La section suivante propose un aperçu des premières phases du processus de classification des données. Elle ne se substitue pas à la mise en œuvre systématique des normes en matière de sécurité de l'information ou des exigences légales découlant d'instruments spécifiques, mais vise plutôt à offrir une compréhension globale des principales étapes nécessaires à l'élaboration et la mise en œuvre d'un système de classification des données. Il existe quatre étapes principales :

|Audit|

•Inventaire des actifs de données

La première étape de la classification des données au sein d'une organisation consiste à procéder à un inventaire des données ou à un « audit des données ». Cette étape doit permettre une compréhension générale des types de données et des informations traitées au sein de l'organisation, de leur valeur, de leur sensibilité et de leur caractère critique.

Cette phase comprend également l'identification des exigences légales applicables et l'audit des politiques et procédures organisationnelles ou administratives existantes en matière de gestion des données, y compris des rôles et responsabilités organisationnels existants en matière de traitement des données.

•Évaluation des risques

D'après la définition des politiques de classification des données, le système de classification des données peut être déployé. L'étape suivante consiste à effectuer une évaluation des risques pour les types de données traitées afin d'identifier et quantifier les risques de gravité et de probabilité, et classer ces risques par ordre de priorité par rapport aux critères d'acceptation des risques et aux objectifs de l'organisation. Le résultat de cet exercice devrait déterminer le choix des mesures

techniques et organisationnelles appropriées à adopter ainsi que les priorités en matière de gestion des risques. Les évaluations des risques devront être périodiques et, de préférence, comparables[6] (sachant que l'environnement technologique et des menaces, de même que les pratiques en matière de sécurité évoluent continuellement au fil du temps).

Le responsable du traitement sera chargé de l'évaluation des risques. Il pourra être, dans certains cas, soutenu dans sa tâche par des exigences légales, comme indiqué dans la section précédente[7]. La loi peut exiger que le responsable du traitement soit en mesure de démontrer que celui-ci est conforme aux exigences et contraintes établies (Procédure réalisée par le GDPR pour le traitement des données à caractère personnel). Voir l'annexe I relative aux considérations sur les facteurs de risque à prendre en compte dans le cadre de ce processus.

•Définir les niveaux de protection et leur application

Des exigences de protection appropriées et regroupées par catégories de classification, devront ensuite être définies pour chaque type d'information.

La quantité de niveaux de classification des données devra être optimale pour l'organisation. Une approche trop nuancée sera difficile à gérer et pourra entraîner un manque d'uniformité dans la protection des données et un risque accru, puis pourra semer la confusion chez les responsables du traitement des données et les sous-traitants. Toutefois, un modèle trop simplifié présente un risque de surclassement ou de sous-classement. Une approche à trois niveaux tend à répondre à la fois aux normes de sécurité de l'information (ISO, NIST et normes nationales) et, dans la plupart des cas, aux attentes en matière de conformité juridique.

•Etablissement des rôles de gestion des données

L'étape suivante consiste à définir les rôles et responsabilités de l'organisation et du personnel en matière de classification et de protection de l'information. Les obligations de gestion des risques propres à chaque rôle devront également être définies. L'objectif est de « traduire » ce qui précède en routines organisationnelles au moyen de politiques et de procédures. Dans le cadre de ce processus, il est également intéressant à ce niveau de réviser et mettre à jour les règlements internes existants.

Finalement, c'est l'organisation, en tant que « responsable du traitement des données » qui sera chargée de la conformité et devra être en mesure de démontrer cette conformité (responsabilité).

|Mise en œuvre|

•Classification

En se fondant sur l'évaluation des risques, le niveau de risque est attribué en tenant compte de chaque objectif de sécurité (confidentialité, intégrité et disponibilité). Une classification globale est attribuée aux données en fonction du facteur le plus élevé[8] . Certains systèmes disposent également d'un niveau combiné (confidentialité élevée, intégrité modérée, faible disponibilité)[9].

6 ISO 27000:2018 ; ISO/CEI 27005 fournit des lignes directrices sur la gestion des risques en matière de sécurité de l'information, y compris des conseils sur l'évaluation des risques, le traitement des risques, l'acceptation des risques, les rapports de risques, la surveillance des risques et leur examen. Des exemples de méthodes d'évaluation des risques sont également inclus.

7 Voir, par exemple, l'article 75 du préambule du RRTP.

8 Classification des données : Adoption sécurisée de cloud. AWS, juin 2018. https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf.

9 Par exemple, IT Grundschutz https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html d'Allemange et ISKE d'Estonie, https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.

•Considérations relatives aux technologies émergentes (Cloud, mobile et IdO)

Une approche fondée sur les risques doit être adoptée pour toutes les évaluations et mises en œuvre techniques, qu'il s'agisse d'équipements traditionnels sur site, d'appareils mobiles, sur le Cloud ou avec des dispositifs de l'Internet des objets (IdO). Les stratégies d'adoption des technologies émergentes devront être influencées par la stratégie de gestion des risques de l'organisation. Néanmoins, elles devront aussi fournir un feedback permettant de mettre à jour la stratégie de gestion des risques de l'organisation à mesure que de nouvelles capacités apparaissent. Une évaluation des actifs de données, des niveaux de risque et des exigences en matière de confidentialité, d'intégrité et de disponibilité devra permettre à l'organisation de comprendre sa tolérance au risque ainsi que les combinaisons acceptables de mise en œuvre, les modèles de service et les emplacements que les technologies émergentes ont à offrir.

En effet, l'une des technologies émergentes les plus méconnues aujourd'hui est le « Cloud ». Lorsque les gouvernements et les organisations ne possèdent pas de programme de classification des données, de processus de gestion des risques et se concentrent sur des contrôles techniques existants plutôt que sur des objectifs de sécurité des données, la crainte, l'incertitude et le doute ont tendance à se propager. Ces dernières empêchent à l'organisation d'adopter des technologies émergentes et de bénéficier de nouvelles capacités, performances et économies.

Une approche de « migration par étapes » peut être utile en ce qui concerne l'adoption des technologies émergentes. Dans ce cas, les actifs et les services sont initialement affectés à des «macro-catégories» (Exemple : non sensibles et non critiques, moyennement sensibles et moyennement critiques, etc…) et une classification détaillée est attribuée à chaque actif et service lors de sa migration vers le cloud[10].

|Contrôle|

•Supervision et assurance qualité

Un directeur des systèmes d'information, directeur des données ou directeur de la sécurité des systèmes informatiques devra être nommée pour la supervision et l'aide, ainsi que pour la révision des décisions de classification. Il sera chargé de la classification des données, des décisions relatives aux risques des données et des mesures de protection requises. Cette personne devra également garantir la qualité de la mise en œuvre des contrôles de sûreté ainsi que la pertinence et l'adéquation des contrôles existants pour atteindre les objectifs de sûreté souhaités et la conformité.

•Amélioration et suivi continus

Après la classification des données, des procédures de sécurité doivent être mises en place en vue d'une surveillance et d'une évaluation constantes afin de continuer à satisfaire aux exigences en matière de gestion des risques et de conformité. Pour atteindre les objectifs de sécurité, il est recommandé d'élaborer des normes et des guides de mise en œuvre en se fondant sur les capacités techniques et non techniques existantes. Ces normes et guides pourront être mises à jour afin de permettre une adoption plus aisée des nouvelles innovations sans qu'une mise à jour de la politique ne soit nécessaire.

10 Sécurité et résilience sur les clouds gouvernementaux : Prendre une décision éclairée. ENISA 2011, https://www.enisa.europa.eu/publications/security-and-resilience...clouds/.../fullReport.

|Révision|

•Révision et ajustement périodiques
Au-delà du contrôle et de l'évaluation continus, des révisions systématiques permettent d'ajuster l'accès aux données et d'examiner les données classifiées. Une méthodologie de reclassement et de révision peut garantir l'application de mesures de sécurité adaptées à la technologie actuelle et à l'environnement menace/risque, mais aussi à l'évolution de la valeur et de la sensibilité des données classifiées. Les informations classifiées devront être révisées régulièrement afin d'éviter le stockage d'informations anciennes, plus couteux et difficile à gérer. Il est également recommandé de revoir de façon périodique les politiques et procédures de classification.

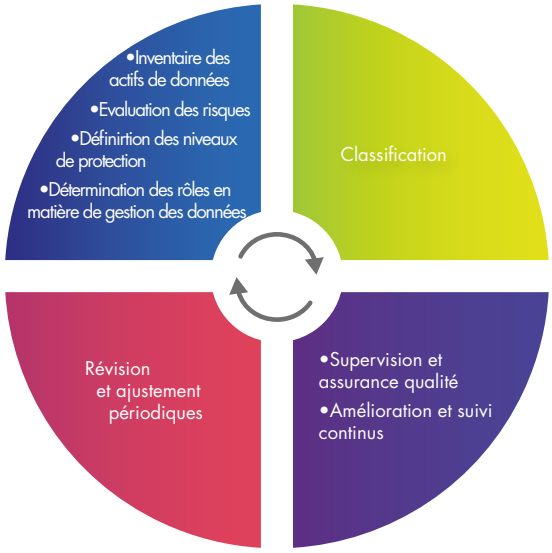

Figure 2- Recommandations pour l'établissement d'un système de classification des données

Ressources recommandées

5

Convention du Conseil de l'Europe sur l'accès aux documents publics (2009) https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084826

Classification des données pour la préparation du cloud. Microsoft, avril 2017. https://gallery.technet.microsoft.com/Data-Classification-for-51252f03

Classification des données : Adoption sécurisée sur le Cloud. AWS, juin 2018. https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

Décret 13526 sur la classification et la déclassification des informations relatifves à la sécurité nationale (CT:IM-226 ; 10-31-2018). Bureau d'origine : A/GIS/IPS https://fam.state.gov/fam/05fam/05fam0480.html ; voir 5 FAM 482.5 pour les catégories de classification.

Guide des bonnes pratiques pour la mise en œuvre sécurisé de clouds gouvernementaux. ENISA, 2013, https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

Règlement général sur la protection des données. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. JO L 119 du 4.5.2016, p. 1-88, http://data.europa.eu/eli/reg/2016/679/oj

Politique de protection de l'information de la CPI, ICC/AI/2007/001. Circulaire du Secrétaire général ST/SGB/2007/6 du 12 février 2007 sur la sensibilité, la classification et le traitement de l'information, https://www.icc-cpi.int/resource-library/Vademecum/ICC%20Information%20Protection%20Policy%20-%202007.pdf

IT Grundshutz. Bureau fédéral de la sécurité de l'information. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Loi sur l'information publique, Estonie https://www.riigiteataja.ee/en/eli/529032019012/consolide

Utilisation sécurisée des services de Cloud dans le secteur financier. Bonnes pratiques et recommandations. ENISA, 2015 https://www.enisa.europa.eu/publications/cloud-in-finance

Loi sur les secrets d'État et les informations classifiées des États étrangers, https://www.riigiteataja.ee/en/eli/501042019009/consolide

Publication spéciale du NIST 800-60 Rev. 1 (Volume 1, Volume 2), Guide pour l'assignation de type d'information et système d'information à des niveaux de sécurité.

Publication 199 sur les normes fédérales du NIST en matière de traitement de l'information : Normes pour les niveaux de sécurité des informations fédérales et des systèmes d'information https://nvlpubs.nist.gov/nistpubs/FIPS/NIST. FIPS.199.pdf

Cadre de gestion des risques (CGR) du NIST) https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

Classification en matière de sécurité du gouvernement britannique https://www.gov.uk/government/publications/government- security-classifications

Organisation internationale de normalisation (ISO) 27001, Exigences relatives aux systèmes de gestion de la sécurité de l'information https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Information Systems Audit and Control Association (ISACA) Objectifs de contrôle pour les technologies de l'information et les technologies connexes (COBIT) http://www.isaca.org/cobit/pages/default.aspx

Blogue de l'AWS sur la résidence des données - https://aws.amazon.com/blogs/security/addressing-data- residency-with-aws/

Livres blancs de AWS - https://aws.amazon.com/whitepapers/

Centre de données et sécurité physique de AWS - https://aws.amazon.com/compliance/data-center/data- centres/

Classification des données de AWS - Adoption sécurisé du cloud Juin 2018 - https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

Annexe I. Scénarios de risque

6

La classification suivante résume les scénarios de risque communément reconnus dans les instruments examinés dans les sections précédentes de ce livre blanc. Plus qu'un catalogue prédéterminé de risques, il peut servir de guide pour l'élaboration d'un système de classification des données aux fins de la gestion des risques découlant des atteintes à la sécurité de l'information (soit confidentialité, intégrité ou disponibilité).

Risques pour la personne	-Impact sur la sécurité physique d'une personne, y compris une menace directe ou indirecte à la vie ou à la santé, quelle que soit sa relation avec l'organisation (personnel ou tiers) ; -Impact sur les droits individuels immatériels (perte ou atteinte à la vie privée, discrimination, atteinte à la réputation ou autre désavantage social important, ou encore privation des droits et libertés d'une personne ou interdiction d'exercer un contrôle sur ses données personnelles) ; -Impact sur les droits et intérêts matériels individuels (lorsque le résultat pourrait être, par exemple, un vol ou une fraude d'identité, une perte financière ou un autre désavantage économique important) ;
Risques pour les activités d'une organisation	-Impact sur le fonctionnement et l'administration efficaces de l'organisation et de ses processus ; -Impact sur la liberté et l'indépendance du processus décisionnel interne et des enquêtes (internes) ;

Risques pour les actifs ou les intérêts commerciaux d'une organisation	-Risque de perte financière pour l'organisation. Impact sur les intérêts financiers de l'organisation ou des autres parties concernées ; -Impact sur les partenaires de l'organisation, y compris sur les informations échangées avec des tiers et considérées comme confidentielles par ceux-ci ; -Impact sur les informations couvertes par le secret professionnel ; -Impact pour l'organisation dans ses négociations commerciales ou politiques ; -Risque pour la réputation, la stabilité ou la sécurité de l'organisation ;
Risque pour la sécurité nationale, l'ordre public ou les relations étrangères	-Impact sur la sécurité nationale et la capacité de défense (y compris les questions technologiques et économiques liées à la sécurité nationale) qui peut porter atteinte aux opérations ou activités de sécurité ; -Impact sur l'exercice des relations extérieures (y compris les informations des gouvernements étrangers) ; -Impact sur l'ordre public et le fonctionnement des autorités de sécurité

Sources et exemples:

GDPR, ISO/CEI, NIST, ICC, droit de la sécurité nationale

(États-Unis, Estonie et pays de l'OTAN/UE).[11]

11 https://www.valisluureamet.ee/nsa/tables.html

— CLASSIFICATION —
DES DONNÉES

OEA | Plus de droits pour plus de personnes

aws

– CLASSIFICATION –
DES DONNÉES

White paper series
Édition 6

2019