LIVRE BLANC

LA CLASSIFICATION DE L'INFORMATION AU SEIN DE L'ENTREPRISE

Enjeux et Démarche pragmatique

LMPS GROUP

NOTRE MÉTIER, **PROTÉGER** LE VÔTRE

AUSIM

Association des Utilisateurs des Systèmes d'Information au Maroc

SOMMAIRE

Mot du Directeur et du Président

L'information revêt pour tout organisme une importance vitale, et doit faire l'objet de mesures de protection adéquates contre toute perte, divulgation, ou utilisation frauduleuse. Dans le contexte économique et technologique actuel, et au regard du volume de plus en plus important d'information généré et traité par les entreprises, La classification est essentielle en tant que socle pour la gestion factuelle de la sécurité de l'information et la maitrise des risques associés.

Le Maroc fait de la sécurité de l'information un levier important du développement national, à travers ses différents plans stratégiques au centre desquels les technologies de l'information jouent un rôle capital. Par ailleurs plusieurs secteurs d'activités se voient encadrés par des dispositions légales et réglementaires qui exigent de la part des entreprises des dispositifs de sécurité adéquats. La mise en place de ces derniers peut se révéler fastidieuse et onéreuse si elle n'est pas priorisée selon la valeur des informations mises en jeu.

La classification permet à l'entreprise d'identifier les informations manipulées au quotidien dans le cadre de ses opérations, et de définir via une analyse des impacts redoutés, les besoins de confidentialité, d'intégrité, de disponibilité de ces informations. Une initiative qui requière la prise en compte des processus essentiels à l'échelle de l'organisme et de tous les types de support d'information (électronique, papier, humain) qui viennent en appui à ces derniers, afin d'en identifier la sensibilité et la criticité.

La classification de l'information fait partie d'un large concept appelé de nos jours la Gouvernance de l'information, qui se présente comme étant un ensemble de structures multi disciplinaires, politiques, procédures, processus et contrôles implémentés afin de manager l'information au niveau des organisations, supportant des exigences à court et long terme d'ordre : réglementaire, juridique, risque, environnementale et opérationnel. La Gouvernance de l'information doit déterminer le point d'équilibre entre deux objectifs potentiellement divergents : extraire de la valeur de l'information et réduire le risque potentiel de l'information. La Gouvernance de l'information réduit le risque organisationnel dans les domaines de la conformité, l'opérationnel, la transparence… Une organisation peut établir un cadre de travail consistent et logique afin de gérer les données à travers les politiques et les procédures de gouvernance de l'information.

L'AUSIM, l'Association des Utilisateurs des Systèmes d'Information au Maroc, en tant que précurseur et dans le cadre de ses missions, s'engage fortement aux côtés des organismes marocains sur toutes les problématiques liées aux systèmes d'information, et en l'occurrence la classification et la sécurité de l'information, objet du présent document.

En collaboration avec LMPS Group, un des leaders en sécurité de l'information dont l'offre couvre toute la chaine de valeur (Processus, technologies, capital humain), l'AUSIM apporte via ce livre blanc une base de compréhension et des lignes directrices aux entreprises souhaitant mener un projet de classification.

Appuyé sur l'expérience internationale de LMPS Group sur le sujet et la sensibilité de l'AUSIM aux préoccupations des organismes marocains, ce livre blanc symbolise l'effort commun des deux organismes et présente les enjeux d'un projet de classification, les facteurs clés de succès, la démarche pragmatique pour sa mise en œuvre et les perspectives une fois le projet réalisé. Nous souhaitons en faire un guide pratique, à l'attention de nos membres, pour la mise en œuvre d'un tel projet.

Très bonne lecture à tous.

Karim HAMDAOUI
Directeur Général de LMPS Group

Mohamed SAAD
Président de l'AUSIM

Introduction

Le contexte économique et concurrentiel actuel fait de l'information l'objet de toutes les convoitises. Cette tendance est renforcée par la multiplication des avancées technologiques en termes d'interconnexion des systèmes, de dématérialisation et de partage de l'information. Au regard des risques encourus, le besoin pour chaque organisme de maitriser les informations entrantes et sortantes est plus que trivial.

La classification des données répond à ce besoin, et constitue par ailleurs la base pour une analyse des risques de sécurité de l'information. Pour réussir la classification des données, il est nécessaire de définir les besoins de sécurité en termes de confidentialité**,** disponibilité et intégrité pour toutes les données et actifs de l'entreprise. Aussi, la granularité de l'information considérée doit être identifiée et maitrisée, afin d'éviter des efforts contre-productifs.

Les informations n'ont pas les mêmes besoins de sécurité et n'obéissent pas aux mêmes règles de protection. Pour les données de certains processus financiers par exemple, au-delà des besoins de confidentialité des données échangées, un fort besoin d'intégrité et de disponibilité est requis pour certaines informations au regard des décisions à prendre, parfois en temps réel, et des montants des transactions en jeux. Le non-respect d'un de ces critères peut avoir des impacts sur les résultats de l'entreprise et provoquer une non-conformité légale et réglementaire.

L'intérêt de la classification est de maitriser les informations transitant au sein de l'entreprise, d'en identifier la sensibilité et la criticité, et définir les dispositions adéquates pour leur protection.

Ce livre blanc, propose une démarche pragmatique pour la classification de l'information et les différentes étapes à suivre pour réussir un tel projet, quel que soit le secteur d'activité et la taille de votre organisme.

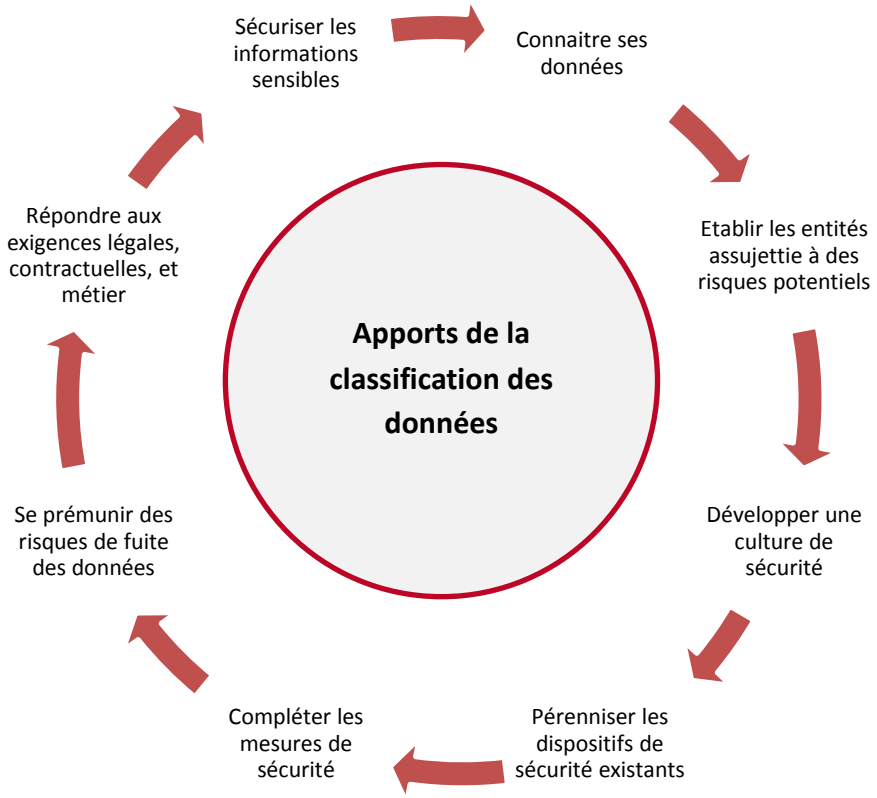
Le coût des violations de sécurité de l'information

Selon le « 2016 Cybersecurity Breaches Survey » au Royaune Uni, 69% des entreprises déclarent que la Cyber sécurité est d'une haute priorité pour le Top Management. 65% des grandes entreprises ont détecté une brèche de sécurité ou une attaque l'année dernière, 25% d'elles sont l'objet d'une attaque par mois. La Stratégie nationale de sécurité des cyber-attaques 2015, a confirmé que les Cyber attaques sont l'une des Top menaces de l'économie du Royaume Uni et à sa sécurité nationale. Suite à la revue de la défense et de la sécurité stratégique, le gouvernement a annoncé un investissement de 1,9 Milliards de pounds dans la cyber-sécurité au cours des cinq prochaines années. Cela inclut la création d'un Centre Cyber National de sécurité en 2016, soit une importante source d'information et de support pour les entreprises du Royaume-Uni sur la cyber-sécurité.

De même selon l'étude faite par le Ponemon Institute LLC en 2016, sur un échantillon de 41 compagnies UK, 2,53 millions de pounds serait le coût moyen des violations des données, avec une progression de 6,5 % sur les deux dernières années.

Pourquoi la classification de l'information ?

La classification est une des étapes prioritaire pour identifier les objectifs de sécurité de l'information pour l'entreprise. Elle permet notamment de mieux maitriser le patrimoine informationnel de l'entreprise et déployer un ensemble de mesures pour sa protection (voir figure ci-dessous).



Les mesures de sécurité et les solutions technologiques de sécurité sont souvent onéreuses pour l'entreprise. La classification de l'information doit, à terme, permettre de guider l'entreprise dans ces investissements et de lui éviter des dépenses superflues.

La classification des données permet en effet de connaître la sensibilité et la criticité de vos informations et choisir les dispositifs de sécurité adaptés pour assurer leur protection. A cet effet, l'identification de l'information et des actifs et la définition des critères de sécurité à considérer est nécessaire. Ces derniers doivent prendre en considération le contexte de l'entreprise, afin d'adapter l'approche pour optimiser la pertinence des résultats.

Par ailleurs, la classification est une

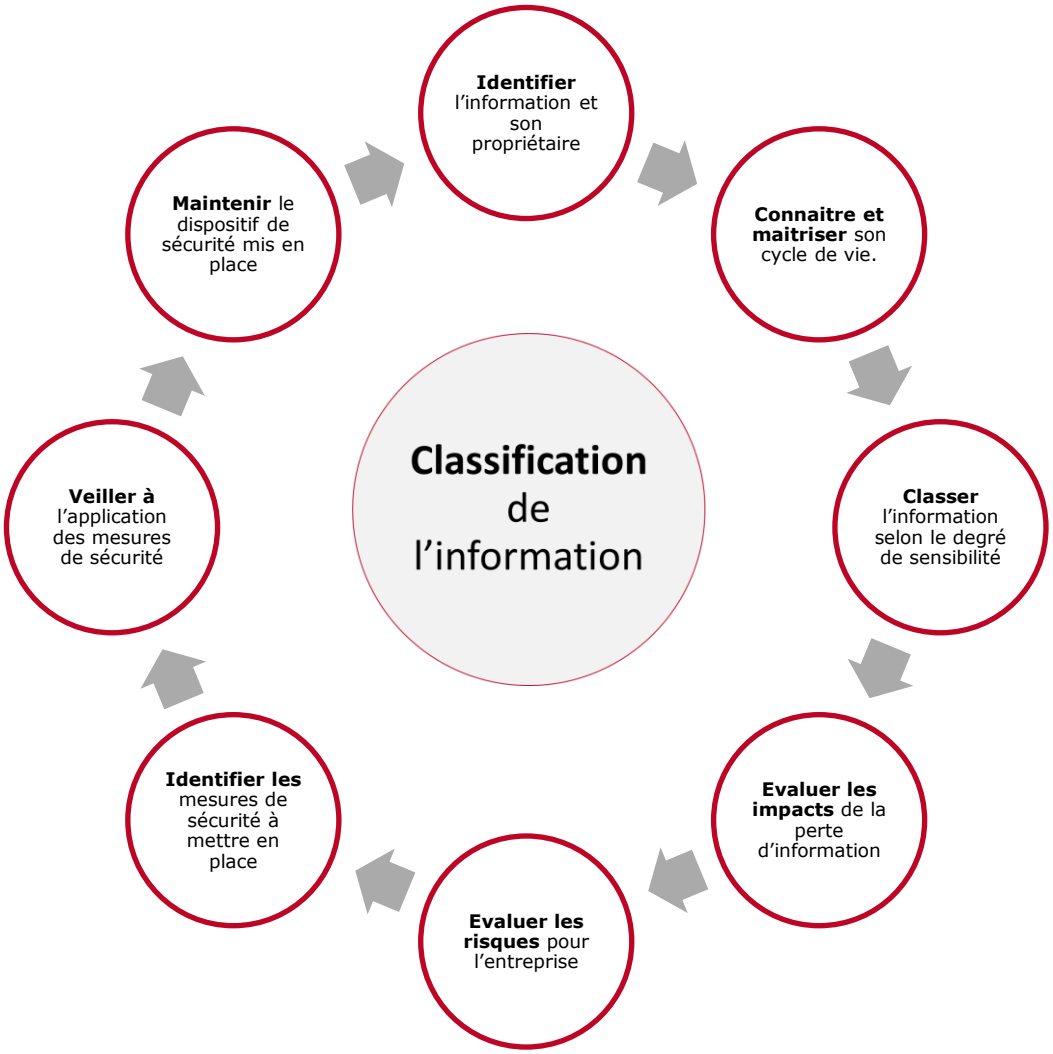
activité indispensable pour la gestion des risques de sécurité dans l'entreprise. Elle permet de choisir les scénarios de risques les plus pertinents, pouvant affecter la capacité de l'entreprise à réaliser ses objectifs de sécurité, et de les évaluer avec précision.

Elle représente ainsi une pierre d'édifice et une brique essentielle pour la gestion de la sécurité de l'information à l'échelle de l'entreprise dans l'optique de la mise en place d'une politique de sécurité de l'information, voire d'un système de management de la sécurité de l'information (SMSI).

Comment classifier l'information ?

L'information est d'une importance capitale pour l'entreprise. Protéger et sécuriser le flux d'information dans l'entreprise demande un effort de toutes les entités métiers et de tous les responsables concernés.

L'approche clé pour une démarche réussie de classification des données, consiste à considérer de bout en bout le cycle de vie de l'information, depuis sa création jusqu'à son archivage ou sa destruction, et considérer les besoins de sécurité (Confidentialité, Intégrité, Disponibilité) à chaque étape du cycle de vie. Ainsi plusieurs priorités se dégagent comme illustré dans la figure ci-dessous :



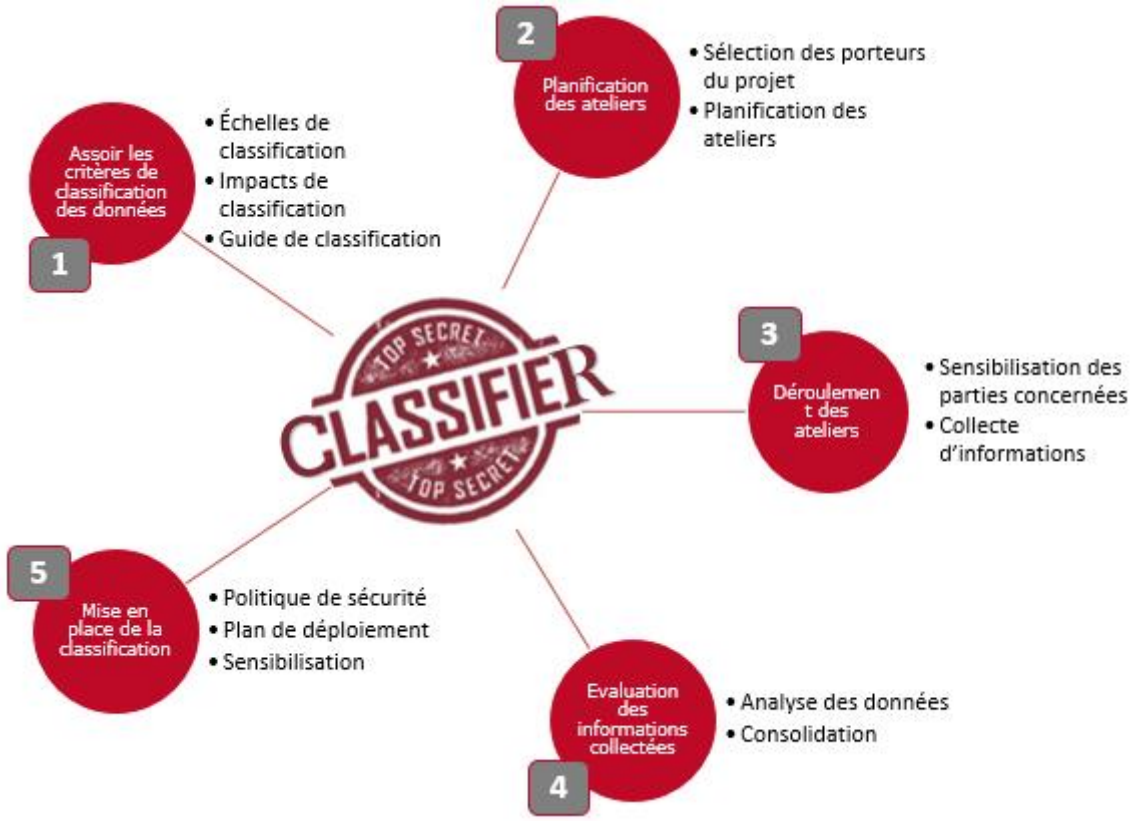
Facteurs clés pour le succès de la classification

La classification des données dépend de plusieurs facteurs. Plusieurs conditions sont essentielles à la réussite d'un tel projet. Dix principaux facteurs clés ont été identifiés et sont décrits dans le tableau ci-dessous :

ID	Facteurs clés	Description
1	**Implication du top management**	La direction générale doit garantir les conditions pour le pilotage du projet de classification, l'implication des parties prenantes, la communication sur le projet, et la mise à disposition des moyens pour le déploiement des règles de protection.
2	**Approche basée sur les processus**	La majorité des entreprises structurent leurs activités en processus. La classification doit s'appuyer sur ces derniers pour rester cohérent au contexte.
3	**Critères de classification pertinents**	Les critères de classification doivent être adaptés au contexte de l'entreprise et validés avant le démarrage des ateliers de classifications. Ces critères portent notamment sur les échelles de classification et les types et niveaux d'impacts redoutés.
4	**Cadrage du projet**	La classification pouvant être fastidieuse, il est recommandé d'aborder un périmètre centré sur les principales activités de l'entreprise. Les processus métier essentiels peuvent être intégrés à ce périmètre initial, ainsi que les activités supports critiques.
5	**Niveau de granularité**	Le volume d'information généré par les entreprises prend de très fortes proportions. Il est primordial d'identifier l'information à un niveau de granularité permettant de rester productif et concentrer les efforts sur l'essentiel, par exemple en groupant les données.
6	**Identification adéquate des parties prenantes**	Les interlocuteurs impliqués doivent avoir les compétences et l'autorité pour se prononcer sur la classification des informations liées à leurs processus.
7	**Collaboration des entités**	Le projet peut se révéler fastidieux selon la taille de l'organisme. La collaboration active des entités est primordiale pour atteindre les résultats escomptés
8	**Qualification du chef projet**	Le responsable de la classification doit être hautement qualifié et avoir une bonne compréhension du métier et des processus de l'entreprise, afin de challenger les niveaux de classification proposés.
9	**Ressources de l'équipe projet**	Les interlocuteurs doivent avoir les compétences et les connaissances nécessaires sur la sécurité de l'information et les processus métier auquel ils sont affectés
10	**Accompagnement par des experts qualifiés**	Le recours à des experts qualifiés permet d'optimiser les délais du projet, garantir l'atteinte des objectifs, et tirer parti de leur retour d'expérience. Le choix de ces derniers doit se faire sur des critères précis d'expérience, de qualifications et de compétences.

Méthodologie de classification de l'information

Pour effectuer la classification des données il est nécessaire de suivre une méthodologie rodée et pragmatique. Cette dernière doit garantir le bon déroulement du projet et permettre de bien cerner les informations à classifier. Il est recommandé à ce niveau du projet de penser à élaborer un guide de classification des données afin d'aider les collaborateurs à assimiler les piliers de la classification et appliquer les critères adoptés pour la réussite du projet et garantir une continuité de classification au sein de l'entreprise.



Les phases principales de la classification des données sont détaillées dans les pages suivantes. Il faut signaler que la sensibilisation est une phase transverse qui doit se dérouler tout au long de votre projet.

Phase 1 : Etablir les échelles de classification

Il ne faut pas oublier que le but de la classification des informations est de garantir la sécurité des données sans entraver la fluidité de l'information et des processus de l'entreprise. Elle s'effectue selon trois critères principaux : La confidentialité, la disponibilité et l'intégrité de l'information. Pour chacun de ses critères, une échelle doit être proposée pour identifier les besoins. Ci-dessous un exemple de description :

Echelle de confidentialité		
Confidentialité	**Description de l'expression de besoin**	**Niveau d'impact redouté**
Confidentiel	Information ayant un impact significatif sur l'organisation si elle était amenée à être communiquée en dehors des personnes nommément désignées.	3
Interne	Information ayant vocation à demeurer au sein de l'organisation. Sa communication hors de l'organisation peut nuire à l'entreprise	2
Public	Information qui peut être rendue publique sans impact redouté pour l'entité ou pour l'organisation	1

Echelle d'intégrité		
Intégrité	**Description de l'expression de besoin**	**Niveau d'impact redouté**
Elevé	Perte d'intégrité intolérable. Toute altération de l'information aurait un impact élevé sur l'entreprise	3
Moyen	Toute altération de l'information aurait un impact important sur l'entreprise	2
Faible	Perte d'intégrité tolérée. Toute altération de l'information aura un impact faible sur l'entreprise	1

Echelle de disponibilité		
Disponibilité	**Description de l'expression de besoin**	**Niveau d'impact redouté**
Elevé	Tolérance à l'indisponibilité très faible. Si ce besoin n'est pas respecté, L'entreprise court un impact élevé	3
Moyen	Tolérance à l'indisponibilité moyenne. Si ce besoin n'est pas respecté, l'entreprise court un impact important	2
Faible	Tolérance à l'indisponibilité élevée. Si ce besoin n'est pas respecté, l'entreprise court un impact faible	1

Ces échelles doivent être personnalisées selon l'entreprise et la nature du métier exercé, afin qu'elles soient adaptées, pertinentes et compréhensibles par l'ensemble des parties prenantes.

Phase 2 : Appréhender les impacts de l'information sur l'entreprise

Plusieurs niveaux d'exposition et de granularité des informations peuvent être identifiés au sein d'une entreprise. Toutes ces informations n'ont pas le même niveau d'impact en cas de divulgation ou d'altération. La connaissance de l'impact permet de prioriser et d'identifier avec plus de précision les activités à risques au sein de l'entreprise, ainsi que les actifs en support à ces dernières (applications, systèmes, équipes, locaux, documents papiers, …)

Les impacts de la perte de confidentialité, de disponibilité ou d'intégrité de l'information sont interliés. Ces impacts peuvent présenter pour l'entreprise des défis pour sa conformité légale réglementaire et contractuelle, ses opérations quotidiennes, sa réputation ou ses finances. Par exemple, la divulgation d'une information confidentielle peut impliquer une perte de confiance dans l'entreprise ou encore des poursuites judiciaires entrainant des pertes financières considérables.

Le tableau ci-dessous apporte une ébauche de description des principaux types d'impacts évoqués.

Impact	4 : Très Grave	3 : Significatif	2 : Modéré	1 : Nul
Conformité	Susceptible d'être considéré comme des infractions systématiques à la réglementation, notamment pour le domaine des systèmes d'information (ex : la loi 09-08, protections des logiciels, fraude informatique, …)	Pouvant être considéré comme une infraction ponctuelle à la réglementation informatique (ex : la loi 09-08, protections des logiciels, fraude informatique)	Susceptible de provoquer un faible nombre de contentieux individuels avec des clients, des partenaires, du personnel ou des tiers.	Aucun impact juridique
	Susceptible de provoquer un grand nombre de contentieux (en série) avec des clients, des partenaires, des personnels ou des tiers.	Susceptible de provoquer un nombre important de contentieux avec des clients, des partenaires des personnels ou des tiers		
Opérationnel	Une altération totale d'un traitement crucial/majeur pour l'entreprise susceptible de provoquer un arrêt ou pendant une durée de l'ordre de 3 jours ou plus (Exemples : paye des collaborateurs, …).	Susceptible de bloquer ou perturber fortement, de façon non planifiée, pendant plus de 24h et moins de 72h le travail de plus de 25% des utilisateurs habituels des applications métiers.	Susceptible de bloquer ou perturber fortement, de façon non planifiée, pendant plus d'une demi-journée et moins d'une journée le travail de plus de 25% des utilisateurs habituels des applications métiers.	Aucun impact organisationnel
	Susceptible d'avoir un impact sur les conditions de travail d'un pourcentage important des utilisateurs (exemple : Introduction de nouvelles technologies, externalisation, …).	Susceptible de créer une surcharge temporaire de travail importante (quelques jours hommes) pour éviter une dégradation significative de la qualité de service rendu		
	Susceptible de créer des mouvements sociaux graves	Susceptible de créer des mouvements sociaux limités		
Réputation	Médiatisation nationale durable	Médiatisation dans la presse publique	Médiatisation dans la presse privée, bouche à oreille négatif	Aucun impact sur l'image
Financier	Coût > 10 000 000 DH	Coûts > 1 000 000 DH	Coûts > 100 000 DH	Coûts < 1000 DH

Les critères choisis (dommage > 100 000 DH, pour les impacts financiers par exemple) doivent être définis selon l'exposition de l'entreprise aux risques considérés, et être validés avec les interlocuteurs concernés, notamment les entités métiers et risques, qui sont rôdés à l'exercice. En effet, un impact grave pour une PME (Petite et moyenne entreprise) peut se révéler nul pour une multinationale. Les conséquences d'une perte de données dépendent de la notoriété de l'organisme, de son périmètre d'action et de son secteur d'activité.

Par ailleurs, l'analyse des impacts redoutés doit tenir compte :

- Du **niveau de granularité** adéquat : préférer les groupes d'information (Dossier du personnel, Dossier de santé, …) contenant l'information classifiée, plutôt que la donnée élémentaire (Nom du collaborateur, numéro de CIN, Numéro de carte, …)

- De l'**étape du cycle de vie** : Considérer le flux de l'information depuis sa collecte (en entrée) par le processus considéré, son traitement par les opérations du processus, jusqu'à son transfert (en sortie) vers les processus en aval. Le besoin en sécurité de l'information peut varier à chacune de ses étapes. Par exemple pour le critère de disponibilité, certains processus ont des périodes critiques, tels que la paie du personnel (fin de mois), les rapports financiers mensuels ou trimestriels. Pour le critère de confidentialité, une nouvelle offre commerciale préparée par une entreprise, passe de la catégorie « strictement confidentiel » ou « Secret » lors de sa préparation, au niveau d'information à caractère publique une fois publiée.

- De la **vision globale à l'échelle de l'entreprise** : Il est nécessaire d'adopter une dualité dans l'approche d'analyse de la classification. Une première approche « Big Picture » (vue globale) permettant d'analyser l'interdépendance des différents processus et les informations échangées à leurs interfaces. Et une deuxième approche « en silos » (vue spécifique) considérant chaque processus et le cycle de vie de son information comme évoqué précédemment.

La prise en compte de ses subtilités est importante pour la pertinence des résultats de classification et la pérennité des dispositifs de sécurité envisagés.

Phase 3 : Classification effective de l'information

Préparation et Planification

Il est nécessaire de planifier adéquatement les ateliers de classification de l'information en coordination avec les principales entités concernées, en identifiant Les interlocuteurs compétents et qualifiés, ayant autorité de décision sur les processus et informations pour lesquels ils sont sollicités.

L'objectif premier des ateliers, est le recueil des informations essentielles de chaque entité afin d'établir une cartographie précise de ces dernières. Avant de commencer ces ateliers de classification, il est nécessaire de s'assurer de la compréhension par les parties prenantes des critères définis (échelles et niveaux d'impact). Il s'agira par la suite d'identifier les informations essentielles aux activités ou processus considéré, puis assister et challenger les interlocuteurs dans l'évaluation des besoins de sécurité pertinents.

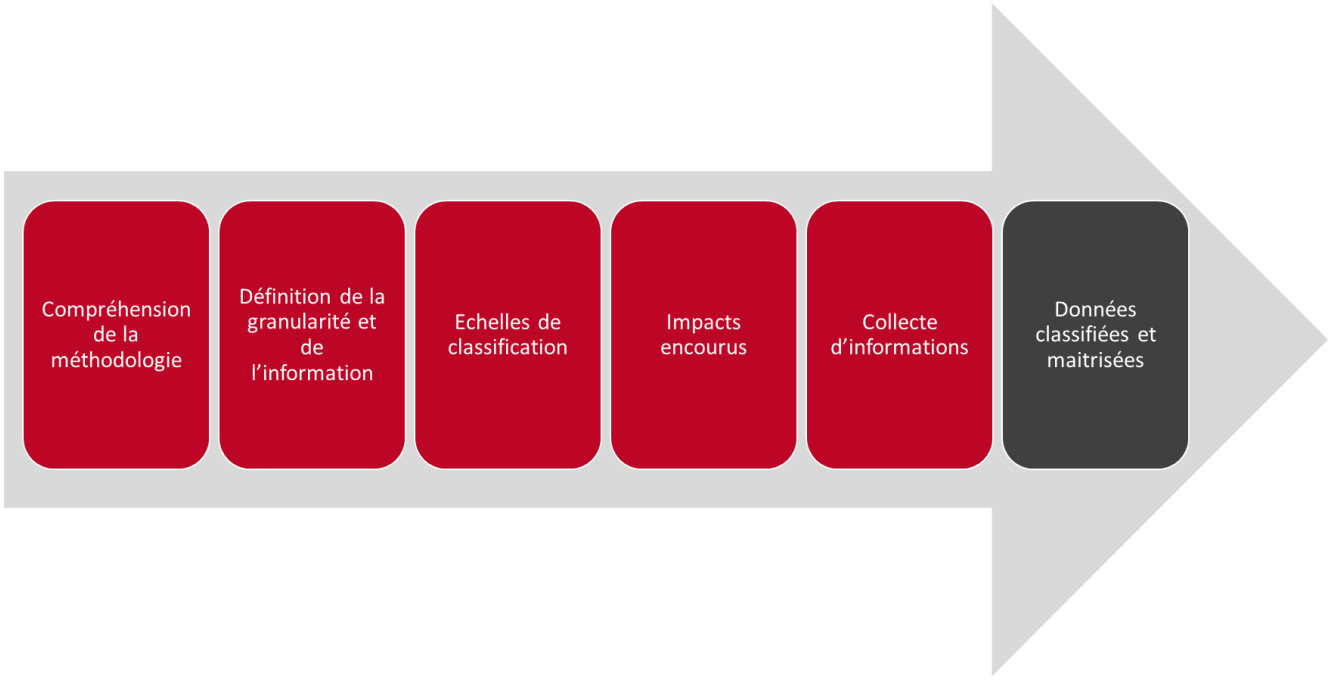
Après avoir identifié les informations essentielles et leur flux au sein du processus ou de l'activité considérés, un ensemble de paramètres doit être identifié, dont les principaux critères suivants :

- **Le nom de l'information :** Pertinent et explicite, pour une identification unique au sein de l'entreprise.
- **Le propriétaire de l'information (Data Owner) :** le responsable de la gestion de l'information.
- **Le format de l'information :** Donnée électronique ou format papier essentiellement.
- **Les responsabilités liées à l'information :** Propriétaire, entités qui y accèdent et droits d'accès.
- **L'impact que l'information peut avoir sur l'entreprise :** Opérationnel, financier, conformité, réputation.
- **Ses besoins de sécurité :** En termes de confidentialité, disponibilité, intégrité.
- **Les canaux de diffusion :** Les SIs sollicités, les systèmes et réseaux par lesquels l'information transite.
- **Les règles de marquage applicables :** Lois et règles applicables à l'information.
- **Le cycle de vie de la donnée :** Durée de vie en tant que donnée courante, avant archivage.
- **Le support de stockage :** Format de conservation (Base de données, application, salle d'archive, …)
- **La conservation :** Les raisons de conservation et la période de rétention.
- **Le procédé de destruction de l'information :** nécessité ou non de mise en rebut, de recyclage…
- **Les mesures de sécurité appliquées dans l'entreprise :** règles d'authentification, de cryptage, de conservation d'intégrité, de traçabilité appliquées à la donnée.

Cet exercice de recueil d'information doit être appliqué à chaque activité au sein d'une entité.

Déroulement effectif des ateliers :

Mener les ateliers de classification des données est la partie culminante du projet. La réussite du projet dépend essentiellement de cette phase critique. Le rôle du chef de projet est d'animer ces ateliers, et permettre aux interlocuteurs métiers de comprendre la méthodologie de collecte des informations et les assister à identifier les informations essentielle. En l'occurrence certaines informations sont interdépendantes, difficile à identifier, ou peuvent se retrouver en redondance. Il est donc opportun de pouvoir anticiper ces écueils.

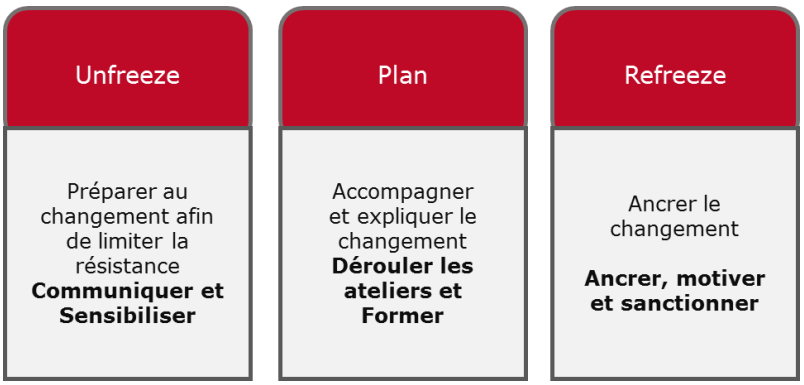


Une fois les données appréhendées, il est nécessaire d'exposer les échelles de classification utilisées aux collaborateurs et responsables présents. Une des règles d'or pour une classification des informations réussie est de bien évaluer la confidentialité, la disponibilité et l'intégrité des données sensibles identifiées pour le processus audité. Une précision à ce niveau est nécessaire tant les collaborateurs et les responsables d'entité ont tendance à considérer que toutes les informations dont ils sont responsables sont secrètes et sensibles. En réalité, les besoins de sécurité de l'information sont très variables entre les informations à leurs dispositions et le rôle du consultant est d'aider les responsables à implémenter une sécurité optimisée pour ne pas handicaper la fluidité du processus.

Par la suite, il faut accompagner l'entité auditée à évaluer les impacts d'une perte de confidentialité, d'intégrité et de disponibilité de l'information. Bien évaluer les impacts de l'information contribue fortement à la compréhension des besoins de sécurité y liés et facilite la collecte des données relatives aux informations sensibles de l'entreprise traitées dans le paragraphe précédent.

Ainsi, grâce à toutes les informations collectées, la classification de l'information se simplifie d'une part, et d'autre part les équipes qui y participent acquièrent une meilleure visibilité sur les informations transitant dans leurs systèmes et prennent conscience de l'importance de la maitrise des données qu'ils traitent. La réussite des ateliers de classification aide indirectement au maintien du dispositif de classification qui sera mis en place par la sensibilisation des donneurs d'ordres et facilite la conduite du changement et l'adoption d'une culture de sécurité dans l'entreprise.

Un des principaux risques projet à surveiller lors de l'implémentation d'un projet de classification des données est la résistance au changement. Il faut traiter de façon proactive ce risque dès le démarrage du projet, et tout au long de sa mise en œuvre à travers le concept « Unfreeze – Change – Refreeze » pour assurer l'atteinte et le maintien des objectifs sur la durée.



En complément sur la problématique de granularité de la classification, il est nécessaire pendant les ateliers d'insister sur l'objectif qui est de classifier l'information et non la donnée élémentaire. L'information, c'est un ensemble de données qui a du sens, et qui se retrouve souvent groupée lorsque les besoins de sécurité se rapprochent, ou lorsqu'elles sont propres à un environnement commun (dossier, base de données, …). Des règles et mesures spéciales peuvent toutefois être nécessaires pour sécuriser des données ayant des besoins de sécurité spécifiquement élevée en raison des exigences métiers, légales ou réglementaires. Pour revenir à l'exemple évoqué dans la section sur les impacts redoutés, dans le cadre du processus des ressources humaines, les informations des collaborateurs sont confidentielles et nécessitent des besoins élevés en confidentialité. Néanmoins, les données de santé, les informations de casier judiciaires, sont plus sensibles (au sens de la loi 09-08 sur la protection des données à caractère personnel) et requièrent par conséquent des mesures supplémentaires.

Aussi, une granularité adaptée de l'information permet d'optimiser les efforts consentis et les mesures à mettre en place pour protéger l'ensemble du patrimoine informationnel.

Analyse et consolidation

Après le recueil des données relatives à la classification, une analyse est nécessaire afin de consolider ces dernières et ressortir les éléments de décision attendus.

Cette analyse est d'autant plus importante qu'elle permet d'épurer l'ensemble des paramètres collectés, d'identifier les redondances ou incohérences éventuelles et mettre en évidence les actifs supports les plus sollicités au sein de l'organisme.

Cette analyse permet aussi de mettre en évidence les éventuels risques opérationnels liés à la mise en œuvre des mesures de sécurité. En l'occurrence, si les niveaux de classification sont excessifs et peu réalistes, les mesures de sécurité pourraient être excessives, réduire la fluidité des processus et impacter les rendements opérationnels. La résistance des équipes à ces changements n'en sera que plus forte.

A l'inverse, si les niveaux de classification sont simplifiés et peu cohérents, l'organisme s'expose à des risques de fuite, d'indisponibilité ou d'utilisation frauduleuse des informations.

La clé, est d'identifier les mesures adéquates et proportionnées, alignée sur les niveaux de classification pertinents, et veiller leur mise en œuvre effective.

Phase 4 : Elaboration de la politique de classification des données

Après collecte, classification et analyse des informations, il est nécessaire de formaliser dans une politique de classification, les règles et les mesures de sécurité à appliquer pour assurer leur protection adéquate.

Cette dernière énonce des règles de classification et propose une approche de mise en œuvre pragmatique des mesures de protection pour chaque niveau de classification et à chaque étape du cycle de vie de l'information. Les mesures peuvent être spécifiées selon le format du support (électronique, papier) afin de renforcer leur caractère pragmatique. La politique de classification, appuyée par le guide de classification évoqué en phase 1, constitue les supports pour garantir le maintien de la classification sur la durée, et l'application au quotidien par chaque collaborateur, des règles énoncées.

Le tableau ci-dessous propose des règles à appliquer à chaque niveau de classification dans le cas du stockage de l'information sur les supports électroniques externes (disques durs, clés USB, …).

Cas d'utilisation		Public	Interne	Restreint	Strictement confidentiel
ACCES AUX DONNEES					
Stockage sur les supports externes	**Règles de sécurité**	Marquage des fichiers	• Sensibilisation des collaborateurs à l'utilisation de supports externes sécurisés • Marquage des fichiers	**Outre les règles des données de type « interne » :** • Utilisation des supports externes éligibles par l'entreprise • Suppression des données immédiatement après leur utilisation • Notification du département Sécurité de l'information en cas de perte d'un support • Chiffrement des données • Utilisation des supports de stockage avec des mécanismes de protection des données	**Outre les règles des données de type « restreint » :** • Création de partition virtuelle cryptée

La politique de classification s'adresse à tout collaborateur devant effectuer la classification des informations et à toute personne concernée par l'utilisation de l'information au sein de l'entreprise (collaborateurs, prestataires, partenaires, stagiaires, …). Elle s'applique aussi bien aux données appartenant aux entités internes, qu'aux données reçues d'entités externes à l'entreprise. Elle doit être réactualisée annuellement afin de rester en adéquation avec les besoins et exigences de l'entreprise.

Phase 5 : Plan de déploiement de la politique de classification

Le plan de déploiement reprend les informations contenues dans la politique de classification des données. Il permet la mise en pratique des mesures de sécurité validées par l'entreprise et aborde le maintien de la classification. Il s'appuie notamment sur les activités suivantes :

1. **Déterminer les paramètres de déploiement**
   - Responsable des mesures de sécurité identifiées ;
   - Echéances de déploiement
   - Ressources nécessaires

2. **Déterminer les rôles et responsabilités minimum pour la classification des données**
   - Les propriétaires de l'information ;
   - Le responsable du suivi et du maintien de la classification
   - La liste des parties prenantes impliquée dans la revue de classification;

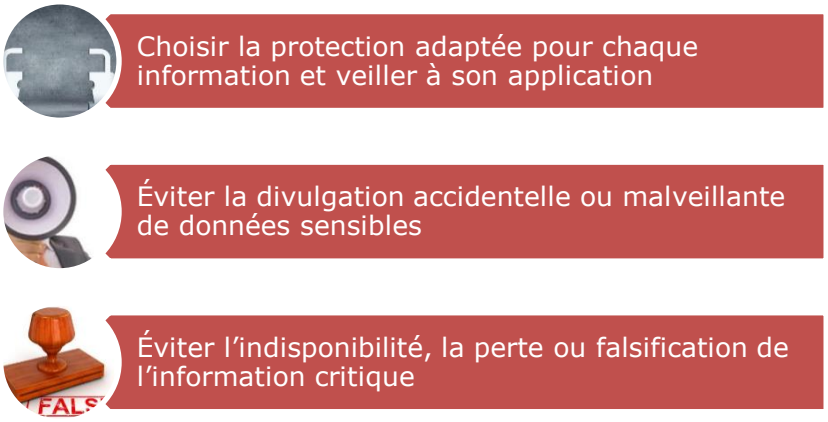
3. **Etablir un plan de sensibilisation continue**

Il est nécessaire de prévoir un programme de sensibilisation et de formation afin de s'assurer que les collaborateurs soient conscients de la nécessité d'éviter les comportements à risque pouvant avoir des impacts préjudiciables pour l'entreprise. Cette sensibilisation doit porter sur les impacts d'une fuite de données, les règles de classification à observer, les mesures de sécurité à adopter. Les acteurs à forte responsabilités peuvent bénéficier de formation sur la classification des données selon les bonnes pratiques du domaine.

Conclusion & perspectives

L'importance de la classification de l'information n'est plus à démontrer, au regard des bénéfices qu'elle apporte en termes d'optimisation des coûts liés à la sécurité et de renforcement des opérations métiers. Il est vivement recommandé pour toute entreprise, quel que soit son niveau de maturité, son secteur d'activité ou sa taille, de faire de la classification de l'information une priorité essentielle et le socle de sa démarche de maîtrise de risques. Pour les organismes matures en termes de sécurité et ayant un ensemble de dispositifs en place, la démarche permettra de remettre en cause ces dispositifs et de les optimiser. Pour les organismes portés sur une première activité de classification, la démarche permettra une meilleure maitrise du flux d'information, et une prise de décision factuelle dans les investissements à consentir pour la sécurité de l'information.

Le patrimoine informationnel est stratégique. La classification des informations permet de :



En tant qu'activité structurante aussi bien pour les opérations de l'organisme que pour la protection de son patrimoine informationnel, le maintien opérationnel de la classification est aussi important que sa mise en œuvre effective. Ce maintien peut être appuyé par des dispositifs tels que :

- Une solution de Prévention contre la fuite de données (Data Leak Prevention - DLP);
- Une analyse des risques de sécurité pour renforcer les mesures de sécurité identifiées ;
- Un système de management de la sécurité de l'information conforme à la norme ISO27001, afin d'aligner l'ensemble aux objectifs de l'entreprise dans une démarche d'amélioration continue.

Document préparé par :

Karim HAMDAOUI, Expert Sécurité, Fondateur LMPS Group
Kevin SIGNE, Consutant Senior Sécurité, LMPS Group
Bassim SENDAGUE, Consultant Sécurité, LMPS Group
Révisé et approuvé par le Bureau de l'AUSIM

Présentation de L'AUSIM

L'Association des Utilisateurs des Systèmes Informations au Maroc (AUSIM) est une association à but non lucratif créée en avril 1993.

Comptant parmi ses adhérents nombre de structures de premier plan aux niveaux organisationnel et managérial (Offices, Banques, Assurances, Entreprises Industrielles, …), l'AUSIM œuvre activement dans l'esprit de développer et de vulgariser l'usage des Technologies de l'Information au Maroc.

A ce titre, elle a pour objectifs :

- L'échange d'expériences et d'informations d'ordre technique, scientifique et culturel entre les adhérents et ce par organisation de rencontres, séminaires et conférences, aussi bien au Maroc qu'à l'étranger,
- L'étude et la sauvegarde, en cas de besoin, des intérêts généraux, à caractères techniques, économiques et financiers de ses adhérents,
- La création et l'entretien des rapports de bonne fraternité entre ses membres et le renforcement des liens avec d'autres associations similaires au Maroc et à l'étranger,
- L'entraide mutuelle au niveau de l'exploitation des systèmes,
- La diffusion des connaissances et d'informations relatives au secteur des technologies de l'Information,
- La participation active aux principales réformes nationales et sectorielles ayant trait aux Technologies de l'Information.

L'Association se compose d'adhérents titulaires et d'adhérents honoraires.

Les adhérents titulaires sont des Administrations, des Sociétés, des Organismes utilisateurs de systèmes d'information à l'exclusion des Sociétés ayant pour activité principale, la vente ou la distribution du matériel informatique. Ils sont représentés par des délégués dûment mandatés.

Les adhérents honoraires sont nommés par l'Assemblée Générale sur proposition du Bureau. Le titre d'adhérent honoraire est conféré comme un hommage à des personnes ou des organismes ayant rendu à l'Informatique ou à l'Association des services éminents.

Présentation de LMPS Group

NOTRE MÉTIER, **PROTÉGER** LE VÔTRE

Depuis sa création en 2007, LMPS Group n'a cessé de répondre aux exigences les plus pointues de ses clients en matière de **gestion des risques**, de **conformité** et **sécurité de l'information**. Fort de son équipe hautement qualifiée, de partenariats mondialement connus, et d'une veille technologique sans relâche, LMPS Group a su se maintenir comme leader de son domaine, à travers ses trois filiales.

LMPS est accrédité PCI QSA « Qualified Security Assessor » par PCI Security Standard Council pour délivrer la certification PCI DSS.

LMPS est certifié ISO 9001 et ISO 27001

www.lmps-consulting.com | www.lmps-technology.com | www.secur-institute.com

PROCESSUS | TECHNOLOGIE | CAPITAL HUMAIN

4, lotissement la colline, BP 92967, 20150
Casablanca – Maroc
Tél : +212 (0) 522 527 785 / Fax : +212 (0) 522 527 789
contact@lmps-group.com / www.lmps-group.com