ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE

DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

GUIDE RELATIF A LA CLASSIFICATION DES DONNEES

Informations

PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :

Rédigé par	Version	Date
DSR	1.0	08/07/2025

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	08/07/2025	Version initiale

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Entités et Infrastructures d'importance vitale (cf. loi n° 05.20 relative la cybersécurité)

POUR TOUTE REMARQUE :

Contact	Email
DGSSI	contact-dsr@dgssi.gov.ma

SOMMAIRE

Introduction

La gestion des données et leur protection sont devenues des priorités pour les administrations et les infrastructures d'importance vitale (IIV) publiques et privées. Avec l'utilisation croissante des technologies de l'information et l'intégration des processus numériques dans les activités de ces organismes, la quantité des données créées et utilisées augmente de façon exponentielle.

Le Maroc, à l'instar des autres pays, est conscient de la nécessité de mettre en place des mécanismes appropriés pour gérer et protéger ses données notamment sensibles. Pour cela, un cadre juridique rigoureux a été mis en place afin de renforcer la sécurité des données et des systèmes d'information en général.

Au cœur de ce cadre se trouve la loi n° 05-20 relative à la cybersécurité, qui constitue l'épine dorsale de l'arsenal juridique du Royaume en matière de cybersécurité. Cette loi prévoit des obligations strictes aux administrations et organismes publics, ainsi qu'aux infrastructures d'importance vitale (IIV). La loi n° 05-20 a mis en place également, via son décret d'application, un référentiel visant à encadrer la démarche de classification des actifs informationnels, y compris des données, et des systèmes d'information des organismes publics et des infrastructures d'importance vitale.

Sur la base de ce référentiel, un premier inventaire des systèmes d'information sensibles pour l'Etat a été dressé. Ces systèmes, qui sont déclarés à la DGSSI, sont soumis à des dispositions de sécurité renforcées.

Conformément au même référentiel, les organismes soumis à la loi 05-20 sont également tenus de procéder à la classification de leurs données et de définir celles ayant un caractère sensible. La classification des données est un exercice préalable à la mise en place des mesures de protection.

Le présent guide est élaboré dans le prolongement de la loi n° 05-20 et de son décret d'application. Il se concentre sur la classification des données en tant qu'actif informationnel à part entière et vise à accompagner les organismes en question dans la conduite de cet exercice de classification.

Le guide offre un éclairage aux entités et aux infrastructures d'importance vitale (IIV) sur les éléments à considérer durant la démarche de classification. Il vise à promouvoir une compréhension commune auprès des acteurs concernés. Le guide est aussi structuré de manière à fournir une vue globale et complète sur les étapes à suivre pour mener à terme le projet. Il a notamment pour objet de :

- Définir les étapes préalables à la classification ;
- Arrêter les principes de base qui encadrent la démarche de classification ;
- Situer la démarche de classification par rapport au cadre global de gestion des données ;
- Clarifier les rôles et les responsabilités des acteurs impliqués dans le processus de classification ;
- Décrire la phase d'évaluation d'impact ainsi que la démarche de classification ;
- Proposer une liste indicative de mesures techniques et organisationnelles pour la protection des données.

I. Cartographie des risques liés aux données

Les données en tant qu'actif informationnel, sont exposées à de nombreux risques qui peuvent compromettre leur sécurité. Ces risques sont multiples et touchent les trois aspects fondamentaux de la sécurité des systèmes d'information : **la confidentialité, l'intégrité et la disponibilité**.

Pour mieux appréhender ces risques et mettre en place des mesures de protection efficaces, il est essentiel d'examiner en détail chacun des trois aspects.

Confidentialité

La confidentialité se réfère à la protection des informations contre tout accès non autorisé. Les données doivent être classées en fonction de leur degré de sensibilité, afin de limiter leur diffusion qu'aux seules personnes habilitées. Une atteinte à la confidentialité peut entraîner des conséquences graves, notamment la divulgation d'informations critiques.

→ *Exemples de risques associés :*

- Espionnage
- Fuites de données
- Vol d'informations
- Perte de données (ordinateurs portables ou supports de stockage égarés, etc.)
- ...

Intégrité

L'intégrité garantit que les données restent exactes et complètes tout au long de leur cycle de vie. Elle prévient toute modification ou falsification non autorisée des informations. La perte de l'intégrité des données peut altérer leur fiabilité, causant des erreurs dans les processus décisionnels et opérationnels.

→ *Exemples de risques associés :*

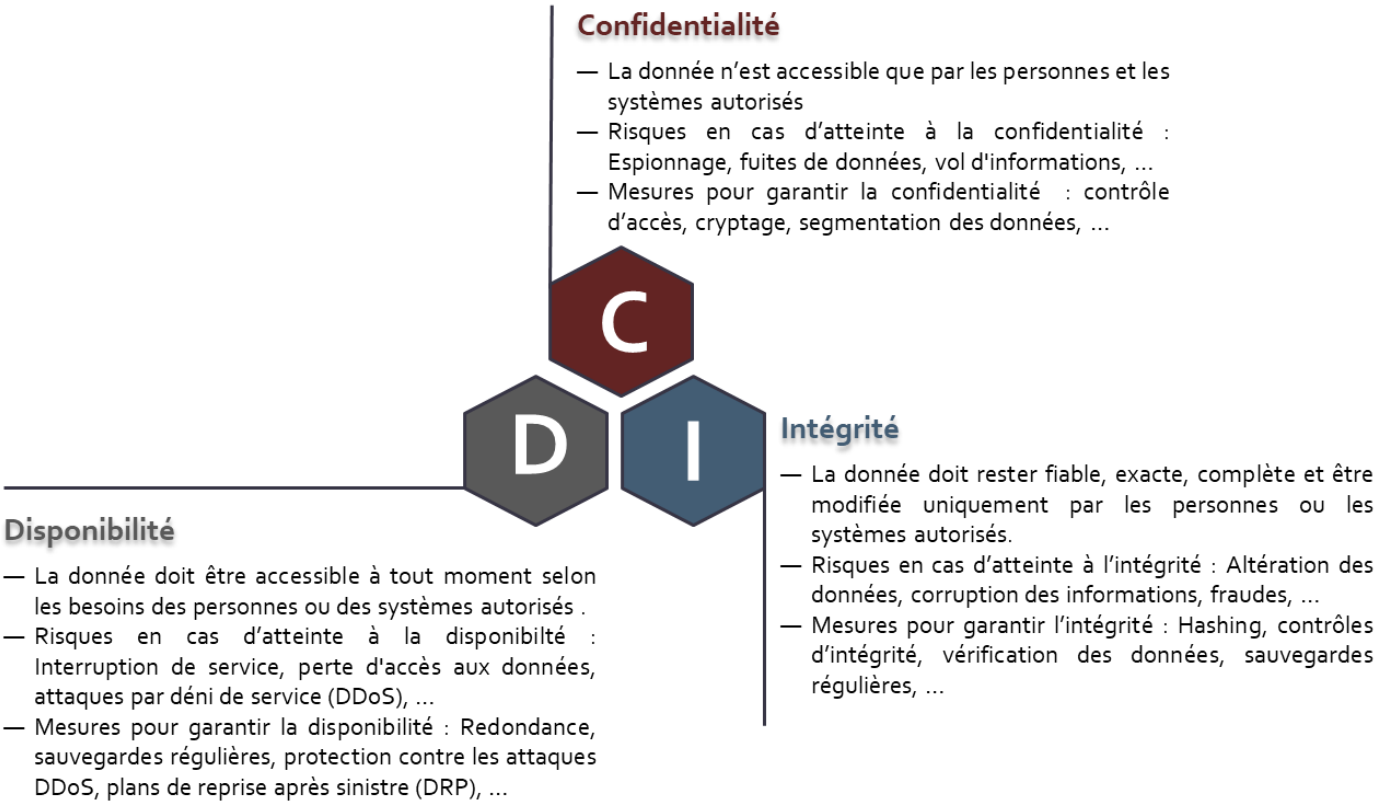
- Manipulation frauduleuse des informations
- Insertion de données non fiables
- Détournement de processus automatisés
- ...

Disponibilité

La disponibilité est le fait que les systèmes d'information et les données soient accessibles et utilisables par les personnes autorisées lorsqu'elles en ont besoin. La continuité des services est un enjeu clé, et toute interruption peut affecter les opérations critiques.

→ *Exemples de risques associés :*

- Attaques par rançongiciels
- Attaques par déni de service
- Catastrophes naturelles (inondation, incendie, tremblement de terre, etc.)
- Suppression de données
- Panne d'équipement
- ...



II. Principes de classification des données

La mise en œuvre d'une opération de classification des données **devrait différer selon le type de l'organisme**. Cependant, certains principes à caractère général sont communs à tous les organismes, abstraction faite de leur importance ou de la nature de leur activité. Ces principes, qui permettent d'encadrer et guider la démarche de classification des données, trouvent leur fondement dans l'arsenal juridique et normatif national régissant la cybersécurité et aussi dans les bonnes pratiques internationales en la matière.

1. Cycle de vie des données

Les données passent par plusieurs phases depuis leur création jusqu'à leur archivage voire leur suppression. **Chaque changement apporté aux données dans le cadre de la gestion de leur cycle de vie impacterait leur niveau de sensibilité et nécessiterait une reclassification**. La valeur des données et leur importance peuvent également changer au fil des années. Certains types de données ont un caractère temporel et leur pertinence ou leur sensibilité peut évoluer avec le temps.

A cette fin, il est nécessaire de garantir que les mesures de protection prennent en considération le statut des données durant leur cycle de vie. Ignorer cet aspect évolutif pourrait donner lieu à des incidents de sécurité.

2. Evaluation des risques

L'objectif recherché à travers la classification des données est de se protéger contre les risques potentiels pesant sur le patrimoine informationnel de l'organisme. Par conséquent, **l'évaluation des risques est un préalable** pour la détermination de la sensibilité et de l'importance des données.

L'évaluation des risques donne lieu, en effet, à la mise en place de mesures de contrôle et de sécurité **proportionnelles** au niveau de risque associé à chaque type de donnée, et ce dans le but d'éviter tout excès ou toute négligence.

3. Proportionnalité

Il s'agit d'assurer un certain équilibre entre la sécurité des données et l'agilité opérationnelle et organisationnelle. L'objectif recherché est de permettre aux organismes de prendre en considération la dimension cyber sécuritaire sans pour autant complexifier les processus métiers ou créer des charges administratives ou financières excessives.

Pour cela, **le niveau de sensibilité attribué aux données doit être, conformément à ce principe, le plus bas possible, mais suffisamment élevé pour assurer une protection adéquate**. Une classification trop élevée risque de limiter l'accès, de créer des contrôles inutiles ou de nuire à l'efficacité organisationnelle. À l'inverse, une classification trop faible peut exposer les données à des risques de cybersécurité, faute de contrôles appropriés.

4. Mise en place d'un cadre de gouvernance

La mise en place d'un cadre de gouvernance approprié est un prérequis pour le succès de toute démarche de classification des données. Il s'agit de créer un environnement où **le processus de classification des données soit mené dans un cadre collégial** et ne repose nullement sur une personne ou une entité.

Pour atteindre cet objectif, il est nécessaire de définir les rôles et responsabilités de chaque intervenant en matière de classification et de protection des données en établissant des procédures précises qui traduisent ces responsabilités en actions et taches concrètes. Lesdites procédures sont appelées à être révisées de manière régulière afin de s'assurer qu'elles restent adaptées à l'environnement des menaces, aux évolutions technologiques, aux exigences réglementaires et aux meilleures pratiques en la matière.

Cette révision périodique a pour but également de s'assurer que les procédures de classification sont alignées avec les objectifs stratégiques de l'organisme.

5. Classification technologiquement neutre et axée sur le contenu

Il s'agit de classer les données strictement en fonction de leur contenu et des risques associés à la compromission de ce contenu, **indépendamment de leur format, support ou origine**. En règle générale, les données, qu'elles soient stockées sur papier, dispositifs numériques, appareils mobiles ou dans le Cloud, doivent être évaluées et classées de manière uniforme.

En privilégiant le contenu plutôt que le support ou la source, les organismes peuvent éviter des incohérences lors de la conception du schéma de protection et qui pourraient survenir si certaines données sont moins bien protégées que d'autres simplement en raison de leur format ou de leur lieu de stockage.

III. Rôles et responsabilités des intervenants dans la classification des données

Le succès de la classification des données dépend de la clarté des rôles et des responsabilités attribués aux différentes parties prenantes impliquées dans le processus. Chaque acteur au sein de l'entité ou l'IIV a un rôle à jouer pour garantir une gestion efficace et sécurisée des données.

Toutefois, les rôles décrits ci-dessous, sont présentés à titre indicatif et ne doivent pas être considérés comme exhaustifs ou impératifs. **Chaque entité ou IIV est invitée à adapter ces rôles en fonction de sa propre structure, de sa taille et de ses besoins spécifiques** afin de répondre au mieux à ses exigences opérationnelles et stratégiques.

Responsable des données (Chief Data Officer)

Le Chief Data Officer est responsable de la gouvernance globale des données au sein de l'entité ou de l'IIV. Généralement rattaché à la direction, il pilote les programmes liés à la valorisation, la protection et la conformité des données. Ses responsabilités incluent :

- **Élaboration de la stratégie Data :** Définir la vision globale de la gestion et de la classification des données, en veillant à son alignement avec les objectifs de l'entité ou de l'IIV.
- **Coordination transversale :** Collaborer avec les différents acteurs (Responsable de la sécurité des systèmes d'information, Propriétaires de données, Dépositaires, Spécialistes de la classification, etc.) pour assurer une cohérence dans la mise en œuvre des politiques de classification.
- **Suivi de la conformité et de la qualité :** Veiller à ce que les pratiques de classification et d'utilisation des données respectent les exigences légales, réglementaires et internes, tout en favorisant leur exploitation optimale.

Responsable de la sécurité des systèmes d'information : il prend en charge la responsabilité de la définition du programme de classification des données dans l'entité ou l'IIV. Ses principales responsabilités incluent :

- Développement de politiques et procédures : Élaborer les politiques et procédures nécessaires pour gérer et classifier les données.
- Surveillance des contrôles de Sécurité : Veiller à ce que les contrôles appropriés soient mis en place pour protéger les données.
- Assignation des rôles : Déléguer et superviser les rôles et responsabilités aux différentes parties prenantes pour une mise en œuvre efficace du programme de classification des données.

Propriétaire des données : il est responsable des données détenues par l'entité ou l'IIV. Ce rôle est généralement attribué aux responsables des unités opérationnelles, qui possèdent une connaissance approfondie de l'importance et de l'utilisation des données. Les responsabilités incluent :

- Évaluation de l'importance des données : Déterminer l'importance des données en fonction des processus métier.
- Classification des données : Assurer que les données sont classifiées de manière appropriée dès leur création.

Dépositaire des données : Il est souvent issu du département des systèmes d'information et est responsable de la protection technique des données. Ses principales responsabilités sont :

- Mise en œuvre des contrôles de sécurité : Appliquer les contrôles de sécurité appropriés en fonction du niveau de classification des données.
- Gestion des accès : Contrôler les accès aux données pour s'assurer qu'ils sont conformes aux politiques de sécurité.
- Surveillance et audit : Effectuer des audits réguliers pour s'assurer que les données sont protégées conformément aux standards de sécurité établis.

Utilisateur des données : Il s'agit de toute personne qui utilise, traite ou manipule les données dans le cadre de ses fonctions. Les utilisateurs doivent être bien informés sur les meilleures pratiques pour la gestion et la protection des données. Des sessions de formation et de sensibilisation peuvent leurs être consacrées. Leurs responsabilités incluent :

- Conformité aux politiques : Suivre les politiques et procédures établies pour la manipulation et la protection des données.
- Signalement des incidents : Signaler tout incident de sécurité ou violation de données à l'équipe de gestion des données.

Spécialiste de la classification des données : il s'agit de l'expert formé pour comprendre les données métier et support et assister les départements dans la classification des données. Ses responsabilités incluent :

- Soutien aux départements : Fournir un support aux différents départements pour assurer la classification correcte des données en ligne avec la stratégie et les politiques de l'entité ou l'IIV.
- Formation et sensibilisation : Conduire des sessions de formation pour sensibiliser les utilisateurs à l'importance de la classification des données.
- Vérification de la classification : Vérifier la classification des données pour s'assurer qu'elle est correcte et conforme aux normes.

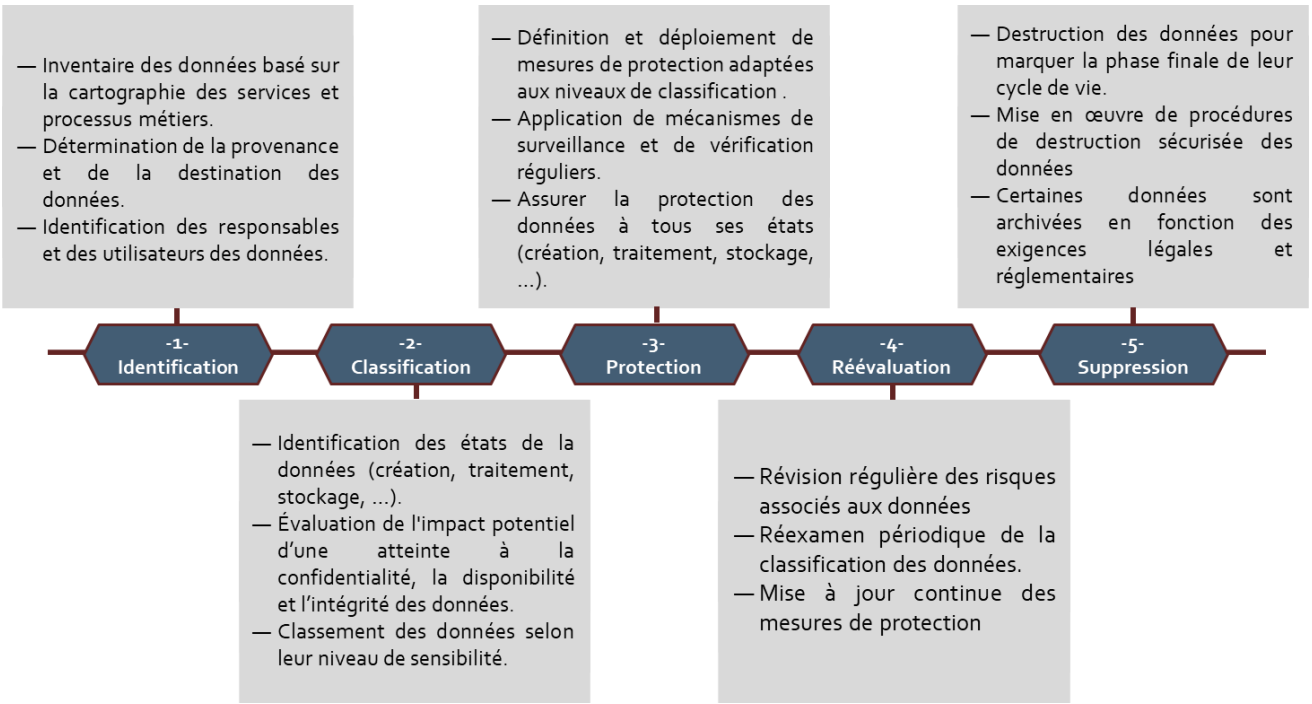
Auditeur des données : L'Auditeur des Données est chargé de revoir la classification des données et de vérifier la conformité aux exigences réglementaires et organisationnelles. Ses principales responsabilités sont :

- **Revue des contrôles de sécurité :** Évaluer les contrôles de sécurité mis en place pour protéger les données.
- **Alignement sur les politiques :** S'assurer que l'utilisation des données est alignée avec les politiques et procédures de protection des données.
- **Suggestions d'amélioration :** Proposer des améliorations pour optimiser la gestion et la sécurité des données.

IV. Processus global de gestion des données

La classification des données n'est ni un acte isolé ni définitif. Elle fait partie intégrante, d'une part, d'un processus global de gestion, et elle est révisable et évolue, d'autre part, en réponse aux changements du contexte opérationnel et des exigences réglementaires. Les données peuvent en effet être reclassifiées, archivées ou même supprimées lorsque leur utilité ou leur pertinence n'est plus d'actualité.

Le processus global de gestion des données est **composé de cinq phases itératives, dont la classification**.



1. Identification des données

La première phase consiste en un inventaire détaillé des données. Pour ce faire, il est important de se baser sur la cartographie des services et des processus métiers qui supportent l'activité de l'organisme. L'objectif est de disposer d'une visibilité complète sur les données disponibles et de cerner leurs flux, en identifiant les ensembles de données utilisés en entrée, les traitements appliqués et les données produites en sortie pour chaque processus ou service.

2. Classification des données

Une fois les données identifiées, la phase suivante consiste à les classifier selon leur niveau de sensibilité et d'importance. En substance, il s'agit d'attribuer à chaque donnée une classe de sensibilité qui reflète sa valeur et les risques associés à sa compromission ou son utilisation inappropriée.

Le chapitre suivant définit les étapes à suivre pour mener à bien une opération de classification des données.

3. Protection des données

Cette phase a pour objet de définir et de déployer des mesures appropriées de protection en adéquation avec le niveau de classification, et ce dans le but de les protéger contre toute compromission de leur confidentialité, intégrité et disponibilité.

Les mesures en question se rapportent notamment au contrôle d'accès, aux sauvegardes régulières, à la traçabilité des accès et des modifications, à la sécurité des locaux où les données sont stockées ou traitées ainsi qu'au chiffrement. Chacune de ces mesures doit être appliquée pour s'assurer que les données, abstraction faite de leur état (au repos, en transit ou en traitement), reçoivent un niveau de protection conforme à leur classification.

Une liste indicative des mesures techniques et organisationnelles de protection des données fait l'objet de l'annexe I.

4. Réévaluation des données

Il s'agit d'une phase de contrôle et de suivi, où les données sont périodiquement réexaminées pour vérifier si leur classification initiale demeure appropriée. En effet, la réévaluation a pour objectif d'ajuster la classification des données en fonction des changements. Si une reclassification s'impose, il est nécessaire de revoir les mesures de protection qui leur sont appliquées, afin de s'assurer qu'elles correspondent au dernier niveau de sensibilité attribué.

5. Suppression des données

La suppression constitue la phase finale du cycle de vie de certaines catégories de données. L'organisme est censé détruire ces données de manière irréversible dès lors qu'elles ne correspondent plus aux objectifs initiaux de leur collecte ou pour se conformer à des exigences législatives ou réglementaires. Cette opération devrait être menée via des méthodes qui empêchent toute récupération ultérieure.

Afin de se conformer à des exigences légales et réglementaires, certaines catégories de données peuvent faire l'objet d'archivage. Dans ce cas, leur suppression doit intervenir à l'expiration des délais de conservation.

Les données archivées font partie intégrante du processus global de gestion des données.

V. Processus de classification

Après avoir situé la classification dans le processus global de gestion des données, ce chapitre met en exergue les étapes nécessaires pour mener à bien un projet de classification. L'objectif est de guider les organismes dans la conception et le déploiement d'une opération de classification des données, allant de la préparation du projet à l'exécution et à la consolidation des résultats.

Il sied de noter que **les étapes de la classification peuvent être adaptées en fonction du contexte de chaque organisme**.

1. Préparation du projet de classification

Cette étape consiste notamment à former l'équipe de projet, à analyser le contexte, à établir une grille des niveaux d'impact et à définir le périmètre opérationnel du projet. L'objectif recherché est de s'assurer que toutes les conditions préalables sont réunies pour une conduite fluide et sans encombre du projet.

→ **Phase 1 : Organisation du projet :**

Le projet de classification devra s'appuyer sur une équipe de projet composée, en plus du chargé de projet désigné, du responsable de la sécurité des systèmes d'information (RSSI) et des représentants des entités métier. L'équipe de projet pourrait faire appel à des consultants ou à des experts externes pour accompagner et renforcer les capacités de ses membres.

Cette équipe sera responsable notamment de :

- La planification des activités et l'échéancier de travail ;
- Le recueil des renseignements requis ;
- L'organisation et l'animation des entrevues et des ateliers de travail ;
- La production des documents de travail ;
- La consolidation et la présentation des résultats.

Les rôles et les responsabilités des acteurs impliqués dans l'opération de classification sont détaillés ci-dessous.

→ **Phase 2 : Analyse du contexte**

Au cours de la phase 2, l'équipe de projet procède à la collecte et à l'examen de toute documentation pertinente lui permettant de délimiter le périmètre de la classification et de définir l'échelle d'impact spécifique à l'organisme (phases 3 et 4). L'analyse effectuée devrait couvrir plusieurs dimensions clés, telles que la taille de l'organisme, ses missions, son domaine d'activités, ses exigences métier, les enjeux de sécurité ainsi que les obligations légales, règlementaires, contractuelles et normatives qui lui sont applicables.

→ **Phase 3 : Définition d'une échelle d'impacts**

Cette phase consiste en la définition d'une échelle d'impacts adaptée qui reflète avec précision les risques spécifiques auxquels l'organisme est soumis, et ce en se basant sur les conclusions de l'analyse du contexte.

L'exercice de classification envisagé par la suite devrait être réalisé conformément à l'échelle d'impacts définie, qui est propre à l'organisme et adaptée à son contexte.

Un deuxième exercice de classification devrait également être mené sur la base de l'échelle d'impacts fixée par la loi 05-20 et son décret d'application, qui est destiné à identifier les systèmes d'information sensibles et les données sensibles pour l'Etat.

En effet, le référentiel de classification des actifs informationnels et des systèmes d'information, préconisé par la loi n° 05.20 et son décret d'application, définit une échelle d'impacts permettant d'identifier les systèmes d'information sensibles et les données sensibles au sens de la loi précitée.

Chaque niveau d'impact de cette échelle fait l'objet d'une description dans l'annexe II, accompagné d'exemples donnés à titre purement indicatif.

→ **Phase 4 : Définition du périmètre de l'exercice de classification**

Il s'agit de déterminer les structures organisationnelles et les processus métiers qui seront concernés par l'exercice de classification. En tenant compte de la taille de l'organisme, cet exercice peut être segmenté en divisant le travail par domaines d'activité. Cette approche permet d'assurer une gestion ciblée et adaptée aux spécificités de chaque domaine.

2. Mise en œuvre du projet de la classification

Après avoir établi les prérequis du projet de classification, l'étape suivante consiste en la mise en œuvre concrète de ce projet. Cette étape se décompose en deux phases :

→ **Phase 1 : réalisation d'un inventaire des données**

Cette phase initiale vise à recenser systématiquement toutes les données faisant partie du périmètre de classification, précédemment défini lors de la phase 4 de la première étape. Pour ce faire, il serait judicieux de programmer des ateliers de travail qui réunissent l'équipe de projet et les responsables des structures administratives ou des processus métiers concernés. Ces sessions de travail ont notamment pour but d'associer toutes les données, qui seront recensées, à leurs propriétaires respectifs ainsi qu'aux processus qu'elles soutiennent ou aux entités auxquelles elles appartiennent.

→ **Phase 2 : Attribution des niveaux de classification**

Il s'agit d'évaluer les impacts potentiels des incidents qui pourraient affecter la confidentialité, la disponibilité ou l'intégrité des données recensées. Cette évaluation devrait se faire conformément à l'échelle d'impacts définie par le décret d'application n° 2-21-406 de la loi 05-20 et, le cas échéant, à l'échelle d'impacts spécifique à l'organisme qui a été arrêté lors de la préparation du projet de classification.

Suite à cette évaluation, un niveau de classification sera attribué à chaque donnée concernée par cet exercice. Pour garantir l'adhésion de toutes les parties prenantes au processus de classification, il est recommandé d'associer les propriétaires des données durant cette phase. Leur participation est essentielle pour assurer que les niveaux de classification attribués reflètent précisément la nature et les risques associés à chaque type de donnée.

VI. Méthodologie de la classification des données (Loi n° 05-20)

Le référentiel de la classification des actifs informationnels et des systèmes d'information aborde la classification des données **sous l'angle de la confidentialité**. Ce chapitre propose d'élargir le périmètre d'analyse en y intégrant également les dimensions d'intégrité et de disponibilité des données, offrant ainsi une méthode exhaustive d'évaluation de leur sensibilité.

Le présent document définit trois échelles distinctes. Chaque échelle permet d'évaluer la sensibilité des données selon l'une des dimensions de sécurité susmentionnées (confidentialité, intégrité, disponibilité).

Pour chaque dimension, l'évaluation en question est réalisée suivant cinq (05) niveaux, allant de zéro à quatre, où le niveau zéro signifie « aucun impact » et le niveau quatre correspond à l'impact « très grave » tel que décrit dans le référentiel précité, objet du décret d'application n° 2-21-406.

Confidentialité	
Echelle de confidentialité	**Description**
Confidentialité_C4	Si un incident de cybersécurité portant sur la confidentialité de la donnée a un impact très grave
Confidentialité_C3	Si un incident de cybersécurité portant sur la confidentialité de la donnée a un impact grave
Confidentialité_C2	Si un incident de cybersécurité portant sur la confidentialité de la donnée a un impact modéré
Confidentialité_C1	Si un incident de cybersécurité portant sur la confidentialité de la donnée a un impact limité
Confidentialité_Co	Si un incident de cybersécurité portant sur la confidentialité de la donnée n'a aucun impact

Intégrité	
Echelle d'intégrité	**Description**
Intégrité_I4	Si un incident de cybersécurité portant sur l'intégrité de la donnée a un impact très grave
Intégrité_I3	Si un incident de cybersécurité portant sur l'intégrité de la donnée a un impact grave
Intégrité_I2	Si un incident de cybersécurité portant sur l'intégrité de la donnée a un impact modéré
Intégrité_I1	Si un incident de cybersécurité portant sur l'intégrité de la donnée a un impact limité
Intégrité_I0	Si un incident de cybersécurité portant sur l'intégrité sur la donnée n'a aucun impact

Disponibilité	
Echelle de disponibilité	**Description**
Disponibilité_D4	Si un incident de cybersécurité portant sur la disponibilité de la donnée a un impact très grave
Disponibilité_D3	Si un incident de cybersécurité portant sur la disponibilité de la donnée a un impact grave
Disponibilité_D2	**Si un incident de cybersécurité portant sur la disponibilité de la donnée a un impact modéré**
Disponibilité_D1	Si un incident de cybersécurité portant sur la disponibilité de la donnée a un impact limité
Disponibilité_D0	**Si un incident de cybersécurité portant sur la disponibilité sur la donnée n'a aucun impact**

Par la suite, une évaluation des impacts doit être conduite sur la base de ces échelles. Le niveau de sensibilité global attribué à une donnée résulte de la combinaison des niveaux de sensibilité identifiés pour chacune des dimensions susvisées.

Concrètement, la donnée reçoit le niveau le plus élevé observé parmi les trois dimensions évaluées. A titre d'exemple, si une donnée est évaluée au niveau 4 en termes de confidentialité, au niveau 2 pour l'intégrité et au niveau 1 pour la disponibilité, elle se verra attribuer le niveau de classification 4.

La matrice ci-dessous explique comment les différents niveaux de sensibilité afférents à chaque dimension de sécurité se conjuguent pour aboutir à un niveau de sensibilité globale.

																Données sensibles									
	C0					C1					C2					C3					C4				
	I0	I1	I2	I3	I4	I0	I1	I2	I3	I4	I0	I1	I2	I3	I4	I0	I1	I2	I3	I4	I0	I1	I2	I3	I4
D0	0	1	2	3	4	1	1	2	3	4	2	2	2	3	4	3	3	3	3	4	4	4	4	4	4
D1	1	1	2	3	4	1	1	2	3	4	2	2	2	3	4	3	3	3	3	4	4	4	4	4	4
D2	2	2	2	3	4	2	2	2	3	4	2	2	2	3	4	3	3	3	3	4	4	4	4	4	4
D3	3	3	3	3	4	3	3	3	3	4	3	3	3	3	4	3	3	3	3	4	4	4	4	4	4
D4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Finalement, en s'appuyant sur une échelle de classification globale, chaque donnée est classifiée de manière à refléter sa sensibilité totale.

Classe	Niveau de sensibilité	Description
Classe I	4	Cette classe est attribuée aux données lorsque l'impact maximal prévu en cas d'incident de cybersécurité affectant la confidentialité, l'intégrité ou la disponibilité est **très grave.**
Classe II	3	Les données sont classées dans cette catégorie lorsque l'impact maximal en cas d'incident de cybersécurité affectant la confidentialité, l'intégrité ou la disponibilité est **grave**.
Classe III	2	Les données sont classées dans cette catégorie lorsque l'impact maximal en cas d'incident de cybersécurité affectant la confidentialité, l'intégrité ou la disponibilité est **modéré**.
Classe IV	1	Les données sont classées dans cette catégorie lorsque l'impact maximal en cas d'incident de cybersécurité affectant la confidentialité, l'intégrité ou la disponibilité est **limité**.
Classe V	0	Cette classe est utilisée lorsque l'incident de cybersécurité n'a aucun impact sur la confidentialité, l'intégrité, ou la disponibilité des données.

Il est à noter que les données de niveaux « C3 » ou « C4 » appartenant à l'une des classes I et II seront considérées des **données sensibles au sens de la loi 05-20 sur la cybersécurité**. Ces données doivent faire l'objet de mesures de protection renforcées, notamment la règle de la résidence sur le territoire national.

Takeaways

- Les données, en tant qu'actifs informationnels à part entière, restent exposées à des risques de cybersécurité susceptibles de compromettre leur confidentialité, intégrité et disponibilité.
- La classification des données est une étape cruciale dans la gestion de la sécurité de l'information. C'est un exercice préalable à la mise en place d'un dispositif de protection. L'objectif d'un exercice de classification est d'identifier et hiérarchiser les données en fonction de leur importance et des risques qui leurs sont associés.
- Malgré la diversité des organismes — eu égard à leur taille, à leur nature ou à leur secteur d'activité — certains principes clés de classification, comme la proportionnalité et la neutralité technologique, demeurent invariables et s'appliquent à tous, indépendamment de leurs contraintes opérationnelles spécifiques.
- Comprendre les menaces et les risques pesant sur les données et appréhender leurs impacts potentiels permet d'attribuer un niveau approprié de sensibilité.
- Le niveau de sensibilité attribué aux données doit être plus bas possible mais suffisamment élevé pour assurer une protection adéquate.
- La classification doit être axée sur le contenu des données et les risques associés à leur compromission, abstraction faite de leur format ou support.

— La classification des données est un processus dynamique et itératif. Il est nécessaire de prendre en compte l'évolution de la sensibilité des données au fil du temps et procéder à une reclassification régulière pour revisiter les mesures de protection, le cas échéant. Cette réévaluation est valable tout au long de leur cycle de vie jusqu'à leur suppression.

— La classification est un travail collégial qui requiert l'implication de plusieurs parties prenantes, notamment les responsables des systèmes d'information, les responsables de la sécurité, les propriétaires des données et les entités métier.

— Pour les organismes soumis à la loi 05-20 sur la cybersécurité, l'exercice de classification doit s'appuyer sur l'échelle d'impacts définie par le décret d'application de la loi et, le cas échéant, sur une échelle d'impacts spécifique à l'organisme, adaptée à son contexte.

— Une méthodologie structurée, comprenant une série d'étapes allant de la préparation initiale à la consolidation des résultats, permet aux organismes de concevoir et déployer une classification efficace et adaptée à leur taille, leur secteur d'activité et leurs contraintes.

ANNEXES :

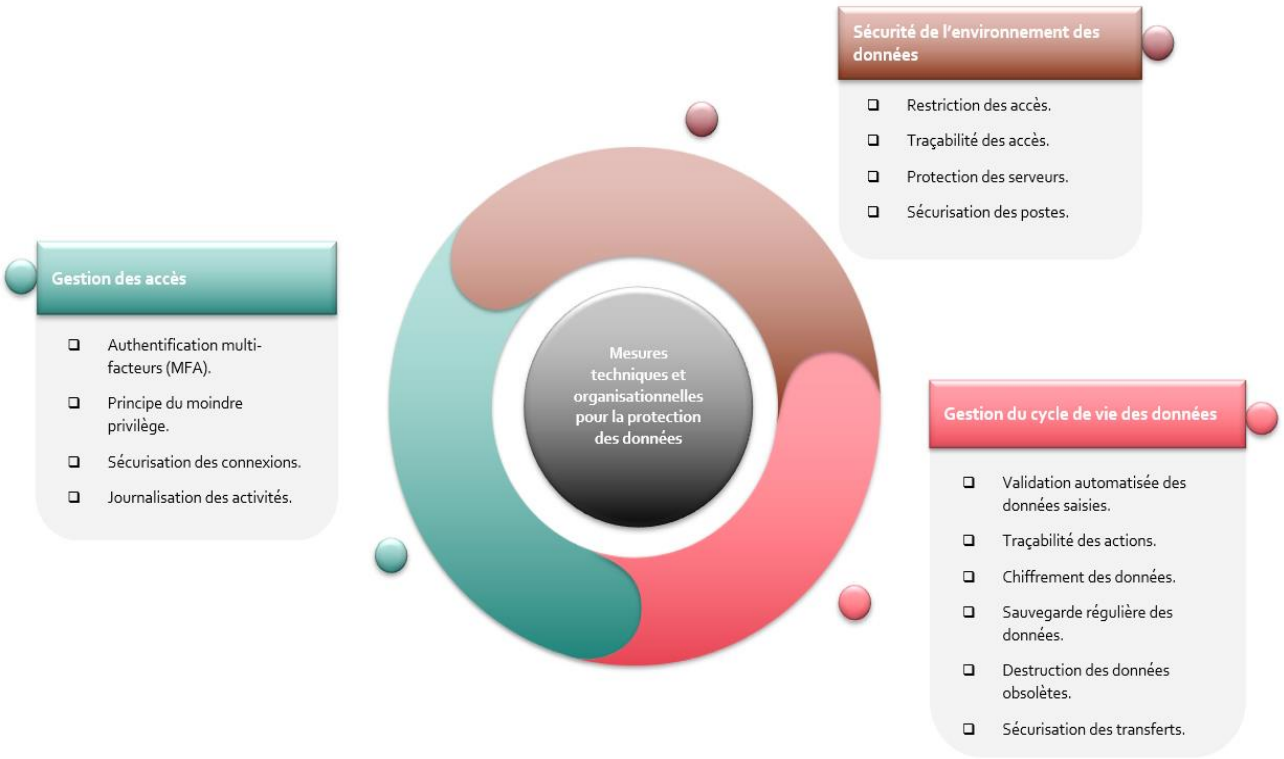
Annexe I : Mesures techniques et organisationnelles pour la protection des données.

Afin d'assurer une protection optimale et appropriée des données, il est nécessaire de mettre en place certaines mesures à caractère technique et organisationnel.

Les mesures techniques concernent directement le système d'information lui-même, tandis que les mesures organisationnelles se concentrent sur l'environnement du système et sur les utilisateurs.

Les deux natures de mesures de protection sont indispensables et complémentaires. Elles permettent de parer à plusieurs risques tel que la destruction, la perte des données, les erreurs, la falsification, les accès non autorisés, etc.

Le schéma ci-après illustre les principales mesures techniques et organisationnelles pouvant être mises en place pour protéger les données. Ces mesures se rapportent notamment à la sécurité de l'environnement des données, à la gestion des accès et à la gestion du cycle de vie des données. Elles doivent être adaptées en fonction du niveau de sensibilité des données et des menaces spécifiques aux technologies utilisées.



Annexe II : Exemples illustratifs pour la classification des données face aux incidents de Cybersécurité.

Les exemples de familles de données présentés par la DGSSI dans cette annexe sont fournis à titre indicatif et ne présentent en aucun cas une attribution définitive d'un degré de sensibilité à ces données. Il s'est agi uniquement d'imaginer un certain nombre de situations et de cas possibles.

Il reste entendu que la classification définitive relève notamment de la responsabilité du propriétaire des données et dépend d'une évaluation détaillée des risques, incluant une analyse approfondie des données et la prise en considération d'autres éléments et facteurs spécifiques au contexte de l'entité ou de l'infrastructure d'importance vitale.

Impact très grave		
Dimension de sécurité	**Description**	**Exemples de Données**
Disponibilité	Données pour lesquelles le délai de récupération en cas d'incident de cybersécurité doit être extrêmement court et dont l'atteinte à la disponibilité pourrait impacter : - Le maintien des capacités de sécurité et de défense de l'État ; - Les intérêts stratégiques de l'État ; - La santé et à la sécurité de la population ; - Le fonctionnement de l'économie nationale ; - La capacité totale ou partielle de plusieurs infrastructures d'importance vitale à assurer leurs fonctions essentielles.	- Données relatives aux infrastructures gouvernementales dont l'indisponibilité pouvant mettre en péril le déploiement des forces, la coordination des réponses d'urgence et la gestion sécuritaire du territoire national. - Archives et documents relatifs à la souveraineté nationale. - Données opérationnelles des systèmes de connexion interbancaires dont l'indisponibilité pourrait perturber les transactions financières, menaçant l'activité économique et la continuité des services bancaires. - Données nécessaires au fonctionnement et à la gestion des infrastructures énergétiques, où toute interruption pourrait affecter la distribution de l'énergie et perturber d'autres infrastructures vitales et l'économie de manière générale. - Données relatives à la gestion du trafic aérien et à la sécurité des vols, dont la perte de disponibilité pourrait entraîner des perturbations ou accidents majeurs, impactant la sécurité de la population et l'économie. - Données permettant la coordination des services de secours et de sécurité publique, dont l'atteinte pourrait retarder les interventions en cas d'urgence, mettant en danger la sécurité publique.
Intégrité	Les données, dont la compromission de l'intégrité et de la fiabilité affecterait :	- Données cliniques et de paramétrage de dispositifs médicaux vitaux, dont l'altération

Impact très grave		
Dimension de sécurité	**Description**	**Exemples de Données**
	- Le maintien des capacités de sécurité et de défense de l'État ; - Les intérêts stratégiques de l'État ; - La santé et à la sécurité de la population ; - Le fonctionnement de l'économie nationale ; - La capacité totale ou partielle de plusieurs infrastructures d'importance vitale à assurer leurs fonctions essentielles.	pourrait compromettre directement la santé et la survie des patients. - Bases de données financières, économiques et sociales clés utilisées pour la régulation et le suivi des activités, notamment les données sur la performance économique, les transactions financières, la balance des paiements et la balance commerciale, pouvant induire en cas d'atteinte des décisions erronées et des perturbations du marché. - Les données des systèmes d'interconnexion bancaire, dont la compromission de l'intégrité pourrait entraîner des erreurs dans les transactions financières, déstabiliser le système bancaire et menacer la stabilité économique nationale. - Données de configuration des réseaux de télécommunications dont l'altération ou la modification pourrait compromettre le fonctionnement des équipements. - Données de contrôle des systèmes de traitement de l'eau (filtration) et de régulation de l'électricité (tension électrique…) menacent directement la santé et la sécurité des citoyens. - Données sur la gestion du trafic aérien, où toute altération pourrait entraîner des incidents graves, mettant en danger la sécurité de la population.
Confidentialité	Les données, dont la divulgation ou l'accès non autorisé pourrait mettre en péril : - Le maintien des capacités de sécurité et de défense de l'État ; - Les intérêts stratégiques de l'État ; - La santé et à la sécurité de la population ; - Le fonctionnement de l'économie nationale ; - La capacité totale ou partielle de plusieurs infrastructures d'importance vitale à assurer leurs fonctions essentielles.	- Données relatives aux réseaux de communication utilisés par les services d'urgence, les forces de sécurité et les infrastructures critiques, dont l'accès non autorisé pourrait perturber les communications en temps de crise et affecter la sécurité de l'État. - Plans de réponse nationale aux crises sanitaires dont la divulgation pourrait accroître la vulnérabilité du pays face aux menaces biologiques et aux actes de bioterrorisme - La cartographie des infrastructures d'importance vitales et des systèmes d'information sensibles - Données relatives aux politiques monétaires, aux régulations des marchés et aux transactions interbancaires, dont l'accès non autorisé pourrait déstabiliser l'économie nationale et provoquer des crises financières.

Impact très grave		
Dimension de sécurité	**Description**	**Exemples de Données**
		- Données relatives aux infrastructures critiques, aux plans de réponses d'urgence, aux opérations de sécurité, incluant les stratégies d'intervention et la logistique, susceptibles d'être exploitées par des acteurs malveillants - Données sur les réseaux de stockage ou de distribution d'électricité, de gaz ou de pétrole, où la divulgation pourrait compromettre l'approvisionnement énergétique et affecter plusieurs infrastructures vitales. - Contenus des positions ou des échanges diplomatiques portant sur des questions qui doivent demeurer secrètes.

Impact grave		
Dimension de sécurité	**Description**	**Exemples de données**
Disponibilité	Les données pour lesquelles le délai de récupération en cas d'incident de cybersécurité doit être court et dont l'atteinte à la disponibilité pourrait engendrer : - Une incapacité totale ou partielle d'une infrastructure d'importance vitale à assurer ses fonctions essentielles ; - Une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions essentielles ; - Des pertes financières importantes pour une ou plusieurs entités ou infrastructures d'importance vitale.	- Données de gestion opérationnelle d'une infrastructure minière : Informations sur le contrôle des équipements d'extraction et de traitement, surveillance des flux de matériaux, et indicateurs de performance environnementale. - Données d'une grande banque, incluant les informations financières et les services numériques, nécessitent une disponibilité continue pour garantir la fluidité des opérations et l'expérience utilisateur. - Contenus des plateformes d'apprentissage et d'enseignement des grandes institutions universitaires.
Intégrité	Les données, dont la compromission de l'intégrité pourrait entraîner : - Une incapacité totale ou partielle d'une infrastructure d'importance vitale à assurer ses fonctions essentielles ; - Une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures	- Données des systèmes de régulation d'une grande exploitation minière : Contrôles automatisés des équipements de forage et d'excavation, surveillance en temps réel des conditions de la mine pour assurer la sécurité et l'efficacité. - Données des transactions financières d'une grande compagnies d'assurances : Transactions de paiement des primes, règlements des

Impact grave		
Dimension de sécurité	**Description**	**Exemples de données**
	d'importance vitale à assurer leurs fonctions essentielles ; - Des pertes financières importantes pour une ou plusieurs entités ou infrastructures d'importance vitale.	sinistres, et transferts financiers liés à la gestion des fonds de prévoyance. - Base juridique nationale officielle dont l'atteinte à l'intégrité pourrait compromettre sa fiabilité. - Métadonnées associées à des projets de recherche nationaux d'envergure. - Base de données des diplômes et des certifications accordés par le système éducatif et universitaire national.
Confidentialité	Les données, dont la divulgation ou l'accès non autorisé pourrait causer : - Une incapacité totale ou partielle d'une infrastructure d'importance vitale à assurer ses fonctions essentielles ; - Une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions essentielles ; - Des pertes financières importantes pour une ou plusieurs entités ou infrastructures d'importance vitale.	- Les données géologiques précises, les emplacements des gisements de minéraux, et les analyses de faisabilité d'une grande entreprise minière. - Les données relatives aux transactions financières, aux informations contractuelles d'une compagnie d'assurance. - Brevets en attente, inventions, et manuscrits non publiés qui, s'ils sont divulgués prématurément, pourraient compromettre la capacité d'une institution à sécuriser les droits de propriété intellectuelle.

Impact modéré		
Dimension de sécurité	**Description**	**Exemples de données**
Disponibilité	Les données dont l'indisponibilité temporaire suite à un incident de cybersécurité entraînerait des perturbations mineures sans compromettre le fonctionnement global et pourrait engendrer : - Une gêne ou perturbation mineure dans les fonctions d'une infrastructure d'importance vitale ; - Une incapacité totale d'une ou plusieurs entités non considérées comme	- Données de suivi des tickets de support technique. - Informations sur les horaires d'ouverture et de fermeture des services publics. - Données de gestion des stocks. - Rapports de satisfaction client. - Informations sur les événements à venir.

Impact modéré		
Dimension de sécurité	**Description**	**Exemples de données**
	infrastructures d'importance vitale à assurer leurs fonctions ; - Des pertes financières modérées ou Toute autre conséquence de nature analogue.	
Intégrité	Les données, dont la manipulation ou l'altération pourrait entraîner : - Une gêne ou perturbation mineure dans les fonctions d'une infrastructure d'importance vitale ; - Une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions ; - Des pertes financières modérées ou Toute autre conséquence de nature analogue.	- Données de gestion de projet. - Informations financières. - Détails des processus internes. - Dossiers de conformité, rapports d'audit. - Données de configuration des systèmes IT.
Confidentialité	Les données, dont la divulgation ou l'accès non autorisé pourrait entraîner : - Une gêne ou perturbation mineure dans les fonctions d'une infrastructure d'importance vitale ; - Une incapacité totale d'une ou plusieurs entités non considérées comme infrastructures d'importance vitale à assurer leurs fonctions ;	- Données personnelles des employés ou des clients. - Projets de développement de produits (concepts, études de marché). - Stratégies marketing internes. - Rapports internes sur les performances. - Données non stratégiques issues de la messagerie interne.

Impact modéré		
Dimension de sécurité	**Description**	**Exemples de données**
	- Des pertes financières modérées ou Toute autre conséquence de nature analogue.	

Impact limité		
Dimension de sécurité	**Description**	**Exemples de données**
Disponibilité	Actes entraînant une inaccessibilité temporaire des systèmes ou services, provoquant des perturbations mineures et récupérables avec un retour rapide à la normale après résolution, pouvant engendrer : - Une gêne ou perturbation dans les fonctions d'une entité non considérée comme infrastructure d'importance vitale ; - Des pertes financières limitées ; - Toute autre conséquence de nature analogue.	- Données de gestion de l'assistance clientèle. - Informations sur les réservations en ligne. - Rapports d'activité des employés. - Informations de suivi des livraisons.
Intégrité	Manipulation ou altération des données, entraînant des erreurs mineures dans les opérations sans impact significatif à long terme et pouvant provoquer : - Une gêne ou perturbation dans les fonctions d'une entité non considérée comme infrastructure d'importance vitale ; - Des pertes financières limitées ; - Toute autre conséquence de nature analogue.	- Données de suivi des ventes. - Informations sur les inventaires. - Détails des transactions comptables. - Rapports de performance des employés. - Données de gestion de projet (modifications non autorisées dans le planning).
Confidentialité	Vol ou divulgation de données non sensibles, entraînant une gêne mineure et des ajustements temporaires, mais avec un impact global négligeable sur les opérations et pouvant causer : - Une gêne ou perturbation dans les fonctions d'une entité non considérée comme infrastructure d'importance vitale ; - Des pertes financières limitées ;	- Informations de contact des clients. - Données de feedback client. - Détails de projets internes (documents de brainstorming, notes de réunion). - Informations sur des événements à venir. - Rapports internes de formation.

	- Toute autre conséquence de nature analogue.	

Sans impact		
Dimension de sécurité	**Description**	**Exemples de données**
Disponibilité	Inaccessibilité temporaire n'engendrant aucune gêne, perturbation ou perte financière.	- Archives de bulletins météorologiques anciens. - Annonces d'événements déjà passés. - Annonces de postes déjà pourvus.
Intégrité	Manipulation ou altération des données n'entraînant aucune gêne, perturbation ou perte financière.	- Archives de messages ou d'emails internes sans valeur actuelle. - Anciennes versions de fichiers déjà mis à jour et archivés. - Fichiers temporaires ou caches générés par des applications.
Confidentialité	Vol de données ne causant aucune gêne, perturbation ou perte financière.	- Détails sur les heures d'ouverture des bureaux gouvernementaux. - Informations sur les programmes de bénévolat disponibles au public. - Résumés de projets artistiques exposés dans des galeries. - Dossiers de presse sur des événements culturels. - Annonces de formations ou ateliers ouverts à tous.

Direction Générale De La Sécurité Des Systèmes D'information
Avenue AL Melia, Hay Ryad, Rabat 10102
www.dgssi.gov.ma
contact-dsr@dgssi.gov.ma