Université de Technologie d'Abidjan

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Enseignante: Dr KIE VICTOIRE

Enseignant-chercheur à ESATIC

CHAPITRE IV: Sécurité des données

1. Introduction

Sécuriser un système informatique nécessite de prendre en compte tous les aspects de sa gestion. Cette sécurité passe par le respect de bonnes pratiques et le maintien de l'outil informatique à l'existant quant aux attaques dont il peut faire l'objet.

Afin de garantir que chaque utilisateur du système informatique n'accède qu'aux données qu'il a besoin de connaître, deux éléments sont nécessaires :

- la remise d'un identifiant unique à chaque utilisateur associé à un moyen de s'authentifier : **une méthode d'authentification ;**

- un contrôle a priori de l'accès aux données pour chaque catégorie d'utilisateurs : **une gestion des habilitations.**

- il est nécessaire de procéder **à une journalisation**, c'est-à-dire l'enregistrement des actions de chaque utilisateur sur le système pendant une durée définie

CHAPITRE IV: Sécurité des données

1. Définitions

- **Les données** sont des faits bruts et peuvent être dépourvues de contexte ou d'intention. Par exemple, une commande d'ordinateurs est une donnée. Les données peuvent être quantitatives ou qualitatives. Les données quantitatives sont numériques, c'est-à-dire le résultat d'une mesure, d'un comptage ou d'un autre calcul mathématique. Les données qualitatives sont descriptives. Le « rouge rubis », la couleur d'une Ford Focus 2013, est un exemple de donnée qualitative. Un chiffre peut aussi être qualitatif : elle est descriptive, et non le résultat d'une mesure ou d'un calcul mathématique.

CHAPITRE IV: Sécurité des données

1. Définitions

- **Les informations** sont des données traitées qui possèdent un contexte, une pertinence et une finalité. Par exemple, les ventes mensuelles calculées à partir des données de ventes quotidiennes recueillies pour l'année écoulée sont des informations. L'information implique généralement la manipulation de données brutes pour obtenir une indication de l'ampleur, des tendances ou des modèles dans les données, tout en visant un but précis.
- **Les mégadonnées (Big Data):** fait référence à des ensembles de données tellement volumineux que les technologies de traitement de données conventionnelles n'ont pas la puissance suffisante pour les analyser

CHAPITRE IV: Sécurité des données

1. Définitions

- **Authentification** : l'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

- **Destinataire des données** : toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.

- **Donnée à caractère personnel** : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

CHAPITRE IV: Sécurité des données

1. Définitions

- **Données sensibles** : les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

- **Responsable de traitement** : la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens dudit traitement, sauf désignation expresse par des dispositions législatives ou réglementaires relatives à ce traitement.

- **Traitement de données à caractère personnel**: toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

CHAPITRE IV: Sécurité des données

1. Définitions

- **La gestion des risques** permet au responsable de traitement d'identifier quelles sont les précautions utiles à prendre «au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès»

- **Le cycle de vie des données** présente le processus de production, d'utilisation et de conservation ou destruction des données dans une organisation. Il liste les différentes étapes et les acteurs intervenants. Le cycle de vie des données s'applique à l'ensemble des données des organisations. Il permet de repérer la manière d'utiliser les données en fonction de leurs caractéristiques et de préciser les différents usages des données en fonction de leur spécificité.

CHAPITRE IV: Sécurité des données

2. Pourquoi la sécurité des données est-elle importante ?

La sécurité des données consiste à protéger les informations numériques contre tout accès non autorisé, toute corruption ou tout vol tout au long de leur cycle de vie. Le concept couvre tous les aspects de la sécurité de l'information, depuis la sécurité physique du matériel et des appareils de stockage jusqu'aux contrôles des administrateurs et des accès, en passant par la sécurité logicielle des applications. Les politiques et les procédures organisationnelles en font également partie.

Lorsqu'elles sont correctement exécutées, de solides stratégies de sécurité des données protègent les actifs informationnels des organisations contre les cybercriminels, mais aussi contre les menaces internes et les erreurs humaines, qui sont les principales causes de violation des données à l'heure actuelle.

La sécurité des données implique le déploiement d'outils et de technologies qui donnent à l'organisation une meilleure visibilité sur l'endroit où sont stockées ses données critiques et sur la manière dont elles sont utilisées. Ces outils doivent idéalement offrir des protections comme le chiffrement, le masquage des données et la rédaction de fichiers sensibles.

CHAPITRE IV: Sécurité des données

2. Pourquoi la sécurité des données est-elle importante ?

Défis à relever: Le volume de données que les entreprises créent, manipulent et stockent ne cesse de croître, ce qui rend la bonne gouvernance des données plus nécessaire que jamais.

Aussi, les environnements informatiques sont plus complexes qu'autrefois car ils englobent désormais le cloud public, le centre de données de l'entreprise et de nombreux dispositifs périphériques comme les capteurs de l'Internet des objets (IoT), des robots ou des serveurs distants. Cette complexité augmente la taille du périmètre à surveiller et à sécuriser face aux attaques potentielles.

Parallèlement, les consommateurs sont de plus en plus sensibles aux questions de confidentialité des données et comprennent son importance. Répondant aux attentes du public, de nombreuses réglementations ont récemment été adoptées en matière de protection de la vie privée.

CHAPITRE IV: Sécurité des données

3. Types de sécurité des données

- **Le chiffrement:** Basées sur un algorithme transformant des caractères de texte normaux en un format illisible, les clés de cryptage brouillent les données afin que seuls les utilisateurs autorisés soient capables de les lire. En rendant illisibles les contenus par chiffrement ou tokenisation, les solutions de chiffrement de fichiers et de bases de données sont l'ultime protection des volumes sensibles. La plupart des solutions intègrent également une gestion des clés de sécurité.
- **L'effacement de données:** Plus sûr que la suppression standard des données, l'effacement des données utilise un logiciel pour éliminer complètement des données sur n'importe quel dispositif de stockage. Les données sont rendues irrécupérables.
- **Masquage des données:** En masquant leurs données, les organisations permettent aux équipes de développer des applications ou de faire des formations en utilisant des données réelles. Les informations identifiant les personnes sont alors masquées lorsque cela est nécessaire pour que le développement puisse se faire dans des environnements conformes.

CHAPITRE IV: Sécurité des données

3. Types de sécurité des données

- **Résilience des données**: La résilience désigne la capacité d'une organisation à subir ou à se rétablir de tout type de défaillance, qu'il s'agisse d'une défaillance matérielle, d'une coupure de courant ou d'autres événements affectant la disponibilité des données (PDF, 256 Ko). La vitesse de récupération est essentielle pour minimiser l'impact.

- **Contrôler les accès**: Ce type de sécurité des données comprend la limitation des accès physiques et numériques aux systèmes et données stratégiques. Vous devez notamment vous assurer que tous les ordinateurs et appareils sont protégés par la saisie obligatoire d'informations d'identification et que les espaces physiques sont uniquement accessibles au personnel autorisé.

- **Authentification**: Comme les contrôles d'accès, l'authentification permet d'identifier avec précision les utilisateurs avant qu'ils aient accès aux données. Elle peut prendre la forme de mots de passe, codes PIN, jetons de sécurité, cartes magnétiques ou identifiants biométriques.

CHAPITRE IV: Sécurité des données

3. Types de sécurité des données

- **Sauvegarde et récupération**: Mettre en place une bonne sécurité des données, c'est aussi prévoir un plan permettant d'accéder aux données en toute sécurité en cas de défaillance du système, de catastrophe, ou de corruption ou fuite des données. Vous devez disposer d'une copie des données sauvegardées dans un format distinct du format d'origine, comme un disque physique, un réseau local ou sur le cloud pour pouvoir les récupérer si nécessaire.

CHAPITRE IV: Sécurité des données

3. Principaux aspects de la sécurité des données

L'ensemble des organisations doit respecter trois aspects centraux de la sécurité des données : confidentialité, intégrité et disponibilité.

- **Confidentialité**. Garantit que les données sont uniquement consultées par des utilisateurs autorisés disposant des informations d'identification appropriées.

- **Intégrité**. Garantit que toutes les données stockées sont fiables, exactes et exemptes de modifications non justifiées.

- **Disponibilité**. Garantit que les données peuvent être consultées à tout moment et de manière sécurisée pour répondre aux besoins continus de l'entreprise.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

Les types de données suivants doivent généralement être protégés :

- informations **personnelles** sur les employés et clients ;
- informations **financières** telles que les numéros de carte de crédit, les données bancaires et les états financiers d'entreprise ;
- données **médicales** telles que les soins reçus, les diagnostics et les résultats de test ;
- propriété **intellectuelle** telle que les secrets de fabrication et brevets ;
- données **opérationnelles** telles que des informations sur la chaîne d'approvisionnement et les processus de production.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ Qu'est-ce qu'une information sensible?

Les informations sensibles désignent toutes les données qui, si elles étaient divulguées, pourraient porter préjudice à des personnes ou à des organisations. Ce type d'informations nécessite des mesures de protection strictes en raison de leur caractère intime ou confidentiel. Les données sensibles peuvent inclure des informations personnelles identifiables (PII), des données financières ou des dossiers médicaux.

❑ Les principales catégories d'informations sensibles

Les informations sensibles varient considérablement et relèvent de différentes catégories:

- ***Informations personnelles identifiables (IPI)*** : Les IPI englobent toutes les données permettant de distinguer ou de retracer l'identité d'une personne, telles que le nom, le numéro de sécurité sociale, l'adresse électronique ou le numéro de téléphone.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ Les principales catégories d'informations sensibles

Les informations sensibles varient considérablement et relèvent de différentes catégories:

- ***Informations financières :*** Détails relatifs aux comptes bancaires, aux cartes de crédit ou à d'autres comptes financiers.

- ***Informations sur la santé*** : Il s'agit des dossiers médicaux, des données relatives à l'assurance maladie ou d'autres informations personnelles liées à la santé.

- **Informations sensibles pour l'entreprise** : Données commerciales confidentielles telles que les secrets commerciaux, les données exclusives, les informations opérationnelles ou stratégiques.
- ***Données à haut risque*** : Les informations qui, si elles étaient divulguées, pourraient avoir des conséquences graves et négatives telles que l'usurpation d'identité, la fraude ou même des failles de sécurité.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Exemples d'informations personnelles identifiables (IPI)**

Les IPI désignent toute information pouvant être utilisée pour distinguer ou retracer l'identité d'une personne. Bien que ce terme désigne toute information de nature personnelle, il comprend essentiellement des points de données qui sont propres à une personne et qui, une fois rassemblés, permettent de l'identifier clairement. Les IIP comprennent:

- **Données personnelles** : Il s'agit du nom complet, de l'adresse du domicile, de l'adresse électronique et des numéros de téléphone d'une personne. Même une photographie personnelle peut être considérée comme une IPI dans la mesure où elle se rapporte à une personne spécifique.
- **Numéros d'identification** : Les identifiants uniques tels que le numéro de sécurité sociale, le numéro de passeport, le numéro de permis de conduire, le numéro d'identification du contribuable ou le numéro d'identification du patient sont indubitablement personnels et figurent en bonne place sur la liste des IIP.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Exemples d'informations personnelles identifiables (IPI)**

- **Identités numériques** : Les identifiants en ligne tels que les noms d'utilisateur, les numéros de compte, les adresses IP ou les identifiants d'appareils mobiles font partie des IIP à l'ère numérique.

- **Enregistrements biométriques** : Avec le développement de la sécurité biométrique, les caractéristiques physiologiques uniques utilisées pour l'identification, telles que les empreintes digitales ou les scans de la rétine, font désormais partie du répertoire des IIP.

- **Caractéristiques ou préférences personnelles** : Il peut s'agir d'attributs physiques (taille, poids, etc.) ou de préférences personnelles, telles que les habitudes d'achat d'une personne ou son historique de navigation sur Internet.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Définition de l'information financière et exemples**

L'information financière, comme son nom l'indique, est centrée sur l'aspect financier de la vie d'un individu ou d'une organisation. Pour mieux comprendre l'information financière, examinons ce qu'elle recouvre :

- **Informations bancaires** : Comprend les détails des comptes bancaires, tels que les numéros de compte, les numéros d'acheminement, les types de comptes bancaires (épargne, courant), ainsi que le nom et l'adresse de la banque.
- **Informations sur les cartes de crédit et de débit** : Les enregistrements des transactions financières, les reçus et l'historique des achats font également partie des informations financières.
- **Détails de la transaction** : Les identifiants en ligne tels que les noms d'utilisateur, les numéros de compte, les adresses IP ou les identifiants d'appareils mobiles font partie des IIP à l'ère numérique.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Définition de l'information financière et exemples**

L'information financière, comme son nom l'indique, est centrée sur l'aspect financier de la vie d'un individu ou d'une organisation. Pour mieux comprendre l'information financière, examinons ce qu'elle recouvre :

- **Informations sur les revenus et les impôts** : Informations sur les revenus d'une personne ou d'une organisation, les sources de revenus, les déclarations de revenus, les prestations de sécurité sociale, etc.

- **Informations sur les investissements** : Comprend les détails relatifs aux investissements individuels ou organisationnels, aux actions, aux obligations, aux comptes de retraite ou à toute autre forme de titres.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Signification et exemples d'informations sur la santé**

Il s'agit de données relatives à la santé physique ou mentale d'une personne, y compris la fourniture et le paiement des soins de santé qu'elle a reçus ou qu'elle recevra. L'accès non autorisé ou l'utilisation abusive de ces informations peut entraîner des violations de la vie privée et potentiellement nuire au bien-être de la personne. Les informations sensibles liées à la santé peuvent inclure

- **Antécédents médicaux** : Il s'agit de données complètes sur les maladies passées, les états pathologiques, les interventions chirurgicales, les allergies et les médicaments que la personne a pris ou prend actuellement.

- **Information diagnostique** : Les informations produites par les tests de diagnostic, tels que les rapports de laboratoire, les rapports d'imagerie et autres examens techniques, relèvent de l'information sur la santé.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Signification et exemples d'informations sur la santé**

- **Dossiers de traitement** : Il s'agit des données relatives aux consultations médicales, aux traitements prescrits, aux dossiers thérapeutiques, aux dossiers d'hospitalisation et aux détails des soins de suivi
- **Données relatives à l'assurance maladie** : Informations relatives aux polices d'assurance maladie d'une personne, telles que le numéro de la police, les données relatives aux sinistres et d'autres informations liées à l'assurance.
- **Antécédents familiaux** : Les informations génétiques et familiales sur la santé qui fournissent des indications sur les risques potentiels pour la santé entrent également dans cette catégorie.
- **Informations sur le mode de vie** : Informations relatives aux facteurs du mode de vie qui peuvent influencer la santé, tels que le tabagisme, la consommation d'alcool, les habitudes en matière d'exercice physique et les préférences en matière de régime alimentaire.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Informations sensibles de l'organisation et exemples**

Les informations sensibles des entreprises méritent une attention constante car elles englobent des données qui, si elles sont compromises, peuvent nuire aux intérêts de l'entreprise. La valorisation et la protection de ces données sont cruciales pour maintenir l'avantage concurrentiel, la réputation et la stabilité financière. Il s'agit généralement des éléments suivants

- **Secrets commerciaux** : Il s'agit d'informations uniques qui distinguent votre entreprise, telles que des formules, des processus ou des dessins, et qui ont une valeur économique du fait qu'elles ne sont pas divulguées. Il est important de protéger tous les secrets dans l'ensemble de la chaîne d'approvisionnement.

- **Informations sur les clients** : Les entreprises détiennent souvent des données sensibles sur leurs clients, telles que les coordonnées, les préférences et les informations financières, qui doivent être soigneusement protégées pour maintenir la confiance et respecter la vie privée.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Informations sensibles de l'organisation et exemples**

- **Plans stratégiques et recherche** : Les lancements de produits à venir, les stratégies de commercialisation, les résultats de recherche et les inventions non brevetées sont des actifs précieux qui méritent d'être protégés contre les concurrents.
- **Informations sur les clients** : Les entreprises détiennent souvent des données sensibles sur leurs clients, telles que les coordonnées, les préférences et les informations financières, qui doivent être soigneusement protégées pour maintenir la confiance et respecter la vie privée.
- **Contrats et documents juridiques** : Les contrats signés, les négociations en cours et les autres accords juridiques contiennent des informations confidentielles qui doivent être protégées pour garantir la sécurité juridique et financière de l'entreprise.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Informations sensibles de l'organisation et exemples**

- **Documents financiers** : La santé financière d'une entreprise repose sur la sécurisation de documents tels que les comptes de résultat, les bilans et les rapports d'audit, qui pourraient nuire à sa situation financière en cas de fuite.

- **Les Propriété intellectuelle** : La protection des documents protégés par des droits d'auteur, des marques ou des brevets, afin de conserver les droits exclusifs et d'éviter les reproductions non autorisées ou le vol, est vitale pour les entreprises.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ Types d'informations sensibles

➢ Exemples de données à haut risque

Les données à haut risque constituent l'épicentre du paysage de la protection des données. Il est classé comme tel en raison de la gravité potentielle des conséquences de sa compromission. L'accès non autorisé, la divulgation ou l'utilisation abusive de ces données peuvent entraîner des pertes financières importantes, une atteinte à la réputation ou de graves violations de la vie privée.

- **Numéros d'identification nationaux** : Les détails tels que les numéros de sécurité sociale ou d'autres identifications nationales entrent dans cette catégorie. Ils sont propres à chaque individu et peuvent être utilisés à des fins d'usurpation d'identité ou de fraude financière.
- **Données biométriques** : Les identifiants biométriques tels que les empreintes digitales, l'iris, les données de reconnaissance vocale ou l'ADN sont considérés comme présentant un risque élevé en raison de leur nature unique et immuable.

CHAPITRE IV: Sécurité des données

3. Types de données devant être sécurisés (informations sensibles)

❑ **Types d'informations sensibles**

➢ **Exemples de données à haut risque**

- **Informations juridiques :** Les dossiers judiciaires, les casiers judiciaires, les procédures légales, les règlements et autres données juridiques peuvent être préjudiciables s'ils sont divulgués sans autorisation.

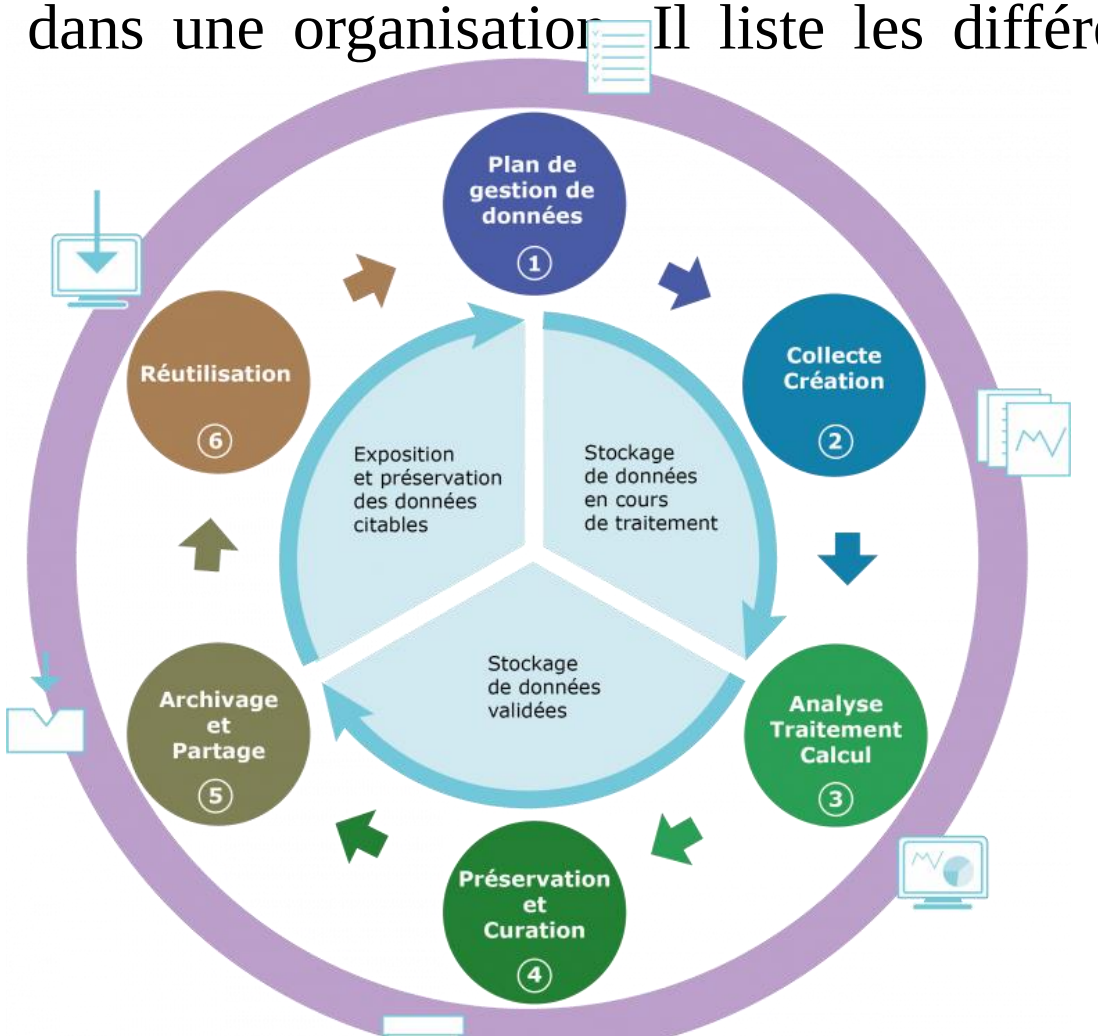
- **Informations gouvernementales sensibles** : Les données confidentielles concernant la sécurité nationale, les opérations militaires ou la collecte de renseignements sont classées à haut risque.

- **Informations sensibles sur l'entreprise** : Secrets commerciaux, informations financières non publiées, plans et prévisions stratégiques, recherches exclusives et autres données commerciales cruciales.

CHAPITRE IV: Sécurité des données

4. Le cycle de vie des données

Le cycle de vie des données présente le processus de production, d'utilisation et de conservation ou destruction des données dans une organisation. Il liste les différentes étapes et les acteurs intervenants.



CHAPITRE IV: Sécurité des données

4. Le cycle de vie des données

- **Collecte de données :**Les entreprises collectent des données à partir de sources fiables, en ligne et hors ligne. Les réseaux sociaux et Internet forment de bonnes sources de grands volumes de données disponibles pour les utilisateurs, gratuites et payantes. Certaines sociétés proposent des informations authentiques basées sur les besoins, ce qui a plus de valeur.
- **Création de données**: Lorsqu'une entreprise débute ses opérations, elle commence à générer et à collecter des informations à grande échelle. Les données de tous ses processus sont enregistrées quotidiennement et stockées numériquement, y compris la fréquentation, l'inventaire, les factures, les réclamations, les requêtes et d'autres transactions.
- **Classification des données**: L'entreprise classe toutes les données collectées et saisies avant leur stockage. La classification facilite le stockage et la récupération efficaces des données. Les grandes entreprises gèrent des bases de données qui stockent les informations par catégorie et offrent de nombreuses installations de traitement, ce qui accroît la valeur des informations.

CHAPITRE IV: Sécurité des données

4. Le cycle de vie des données

- **Archivage des données:** La collecte et le stockage des données sur une période peut représenter un volume important, ce qui complique le tri et l'archivage des informations. C'est pourquoi il est essentiel de documenter et d'archiver régulièrement les données stockées afin de les rendre disponibles lorsque la nécessité l'impose, et de permettre aux requêtes et transactions fréquentes de n'utiliser que les données les plus récentes et pertinentes.
- **Sécurité des données** :Qu'elles soient archivées ou en temps réel, les données doivent être stockées en lieu sûr par les entreprises. La cybersécurité est essentielle pour la protection du cycle de vie de l'information en raison du nombre croissant de menaces dirigées vers la confidentialité des données et d'attaques d'acteurs malveillants dans le monde entier.
- **Suppression des données**: Au fil du temps, les données deviennent obsolètes pour plusieurs raisons, comme l'évolution des processus, la modification des politiques ou l'adoption de meilleures stratégies. Les coûts relatifs aux données obsolètes peuvent être assez élevés pour les entreprises en raison des frais liés à la sécurité des données, mais également des coûts relatifs à leur traitement, leur stockage et à leur récupération.

CHAPITRE IV: Sécurité des données

4. Le cycle de vie des données

- **Affectation des données: L'évaluation** des éléments stockés est essentielle pour pouvoir les utiliser. La gestion des données est coûteuse et nécessite fréquemment une évaluation approfondie. Les entreprises peuvent compiler et stocker des données en vrac à utiliser ultérieurement pour les calculs. Elles peuvent également récupérer et analyser d'anciennes données à des fins de comparaison, pour ensuite identifier des modèles qui aident les décisions de gestion.

CHAPITRE IV: Sécurité des données

5. Menaces pour la sécurité des données

- **Piratage:** Le piratage désigne les tentatives opérées via un ordinateur de vol de données, de corruption de réseaux ou fichiers, de prise de contrôle de l'environnement numérique d'une organisation ou de perturbation de ses données et activités. Les tentatives de hameçonnage, les programmes malveillants, les déchiffrements de code et les attaques par déni de service distribué (DDoS) sont des méthodes de piratage.

- **Rançongiciels** :Les rançongiciels sont des programmes malveillants qui bloquent l'accès à votre réseau et vos fichiers jusqu'au paiement d'une rançon. Ouvrir la pièce jointe d'un e-mail ou cliquer sur une publicité sont quelques-unes des manières dont les rançongiciels peuvent être téléchargés sur votre ordinateur. Ceux-ci sont généralement détectés lorsque vous ne parvenez pas à accéder à des fichiers ou qu'un message exigeant le paiement d'une somme apparaît

CHAPITRE IV: Sécurité des données

5. Menaces pour la sécurité des données

- **Fuite de données:** Une fuite de données est le transfert intentionnel ou accidentel de données depuis l'intérieur d'une organisation vers un destinataire externe. Une telle opération peut être accomplie via les e-mails, l'Internet et les appareils tels que les ordinateurs portables et les dispositifs de stockage portables. Les fichiers et documents récupérés localement sont aussi une forme de fuite de données.

- **Le Hameçonnage:** Le hameçonnage est l'acte d'inciter des individus ou organisations à communiquer des informations telles que des numéros de carte de crédit et mots de passe. L'objectif est de dérober ou d'endommager des informations sensibles en se présentant comme une entreprise respectable que la victime connaît.

CHAPITRE IV: Sécurité des données

5. Menaces pour la sécurité des données

- **Négligence**: La négligence désigne les événements au cours desquels un employé enfreint sciemment une stratégie de sécurité sans cherche à causer un préjudice à l'entreprise. Par exemple, il peut partager des données sensibles avec un collègue qui n'est pas autorisé à y accéder, ou se connecter à des ressources de l'entreprise via une connexion sans fil non sécurisée. Un autre exemple consiste à autoriser une personne à entrer dans un bâtiment sans qu'elle n'ait présenté de badge.

- **Le Vol**: est une menace interne qui peut toucher des données, des fonds ou la propriété intellectuelle. Il est commis à des fins personnelles, dans le but de porter préjudice à l'organisation. Par exemple, un fournisseur connu peut vendre des numéros de sécurité sociale sur le dark web ou utiliser des informations internes sur les clients pour lancer sa propre activité.

CHAPITRE IV: Sécurité des données

5. Menaces pour la sécurité des données

- **Catastrophes naturelles**: Les catastrophes naturelles peuvent arriver sans préavis, aussi est-il judicieux d'effectuer des préparatifs à l'avance pour protéger vos données en pareil cas. Ouragans, tremblements de terre, inondations ou autres formes de destruction, etc., disposer de sauvegardes de vos données hors site vous aidera à mettre en œuvre votre plan de continuité de l'activité.

- **Escroquerie**: Les actes d'escroquerie sont commis par des utilisateurs sophistiqués cherchant à tirer parti de l'anonymat en ligne et de l'accessibilité en temps réel. Ils peuvent créer des transactions à l'aide de comptes compromis et de numéros de carte de crédit dérobés. Les organisations peuvent être victimes d'escroqueries liées à une garantie, un remboursement ou un revendeur.

CHAPITRE IV: Sécurité des données

6. Technologies de sécurité des données

Les technologies de sécurité des données sont des éléments clés d'une stratégie de sécurité des données plus complète.

- **Chiffrement des données**. Utilisez le chiffrement des données (conversion des données en code) sur les données au repos ou en mouvement afin d'empêcher les utilisateurs non autorisés de visualiser le contenu du fichier même s'ils ont accès à son emplacement.

- **Authentification et autorisation des utilisateurs.** Vérifiez les informations d'identification des utilisateurs et confirmez que les privilèges d'accès sont correctement attribués et appliqués. Le contrôle d'accès en fonction du rôle aide votre organisation à octroyer l'accès aux seules personnes qui en ont besoin.

- **Détection des risques internes**. Identifiez les activités susceptibles de révéler la présence d'un risque ou d'une menace interne. Comprenez le contexte d'utilisation des données et déterminez quand certains téléchargements, e-mails à l'extérieur de votre organisation et fichiers renommés sont caractéristiques d'un comportement suspect.

CHAPITRE IV: Sécurité des données

6. Technologies de sécurité des données

- **Stratégies de protection contre la perte de données**. Créez et appliquez des stratégies qui définissent la gestion et le partage des données. Spécifiez les utilisateurs, applications et environnements autorisés pour diverses activités afin d'empêcher la fuite ou le vol des données.

- **Sauvegarde des données.** Sauvegardez une copie exacte des données de votre organisation afin que les administrateurs autorisés aient la possibilité de les restaurer en cas de défaillance du stockage, de violation de données ou de sinistre.

- **Alertes en temps réel**. Automatisez les notifications signalant une mauvaise utilisation potentielle des données et recevez des alertes liées à des problèmes possibles de sécurité avant qu'ils n'endommagent vos données, votre réputation ou la confidentialité de vos employés et clients.

CHAPITRE IV: Sécurité des données

6. Technologies de sécurité des données

- **Évaluation des risques.** Comprenez que vos collaborateurs, fournisseurs, sous-traitants et partenaires disposent d'informations sur vos données et pratiques en matière de sécurité. Pour empêcher le détournement des données, cernez les données dont vous disposez et leur utilisation au sein de votre organisation.

- **Audit des données.** Gérez les principales préoccupations liées à la protection des données, leur exactitude et leur accessibilité à l'aide d'audits planifiés régulièrement. Ceux-ci vous permettront d'identifier les personnes qui utilisent vos données et de quelle façon.

CHAPITRE IV: Sécurité des données

7. Stratégies de sécurité des données

Une stratégie globale de sécurité des données comporte des personnes, des processus et des technologies. L'efficacité des contrôles et des politiques de sécurité dépend autant de la culture organisationnelle que de l'utilisation d'outils adéquats. Cela signifie que la sécurité des informations doit devenir une priorité dans tous les secteurs de l'entreprise.

- **Sécurité physique des serveurs et des appareils des utilisateurs:** Que vos données soient stockées sur place, dans un centre de données d'entreprise ou dans un cloud public, vous devez vous assurer que les installations sont protégées contre les intrus, qu'elles disposent d'un système de sécurité incendie et d'un contrôle de température fiables. Un fournisseur de services cloud assumera ces responsabilités pour vous.
- **Gestion et contrôle des accès**: Le principe du moindre privilège doit être appliqué à l'ensemble de votre environnement informatique. Ainsi, l'accès aux bases de données, au réseau et aux comptes administrateurs n'est accordé qu'à un nombre restreint de personnes, et seulement à celles qui en ont absolument besoin pour leur travail.

CHAPITRE IV: Sécurité des données

7. Stratégies de sécurité des données

- **Sécurité et correction des applications**: Tous les logiciels doivent être mis à jour dès que possible après la publication de correctifs ou de nouvelles versions.

- **Sauvegardes**: La conservation de copies de sauvegarde utilisables et testées en profondeur, de toutes les données critiques, est un des éléments clés d'une stratégie de sécurité des données solide. Il faut en outre appliquer aux sauvegardes les mêmes contrôles de sécurité physiques et logiciels que ceux utilisés pour l'accès aux bases de données primaires et aux systèmes centraux.

- **Formation des équipes**: En sensibilisant les équipes à l'importance des bonnes pratiques de sécurité et de mots de passe et en leur apprenant à reconnaître les attaques reposant sur l'ingénierie sociale, elles deviennent des « pare-feu humains » qui peuvent jouer un rôle essentiel dans la protection de vos données.

CHAPITRE IV: Sécurité des données

7. Stratégies de sécurité des données

- **Surveillance et contrôles de la sécurité des réseaux et des terminaux**: La mise en place d'une suite complète d'outils et de plateformes de gestion, de détection et de réponse aux menaces dans votre environnement sur site et dans le cloud peut limiter les risques et réduire la probabilité d'une violation.

CHAPITRE IV: Sécurité des données

8. Tendances en matière de sécurité des données

- **Surveillance et contrôles de la sécurité des réseaux et des terminaux**: La mise en place d'une suite complète d'outils et de plateformes de gestion, de détection et de réponse aux menaces dans votre environnement sur site et dans le cloud peut limiter les risques et réduire la probabilité d'une violation.

- **IA**: L'IA renforce les capacités d'un système de sécurité des données car elle peut traiter de grandes quantités de données. L'informatique cognitive, une branche de l'IA, effectue les mêmes tâches que les autres systèmes d'IA, mais en simulant des modes de pensée humains. Elle permet une prise de décision rapide en cas de situation critique en matière de sécurité des données.

- **Sécurité multicloud**: La définition de la sécurité des données s'est élargie avec le développement des capacités du cloud. Aujourd'hui, les organisations ont besoin de solutions plus complexes, car elles doivent protéger non seulement les données, mais aussi les applications et les processus d'entreprise propriétaires qui fonctionnent dans les clouds publics et privés.