

# SÉCURITÉ DES DONNÉES & BLOCKCHAIN



DSBD-M1  
2024/2025

Abdelaziz ETTAOUFIK  
Enseignant Chercheur  
FSBM  
[a.ettaoufik@gmail.com](mailto:a.ettaoufik@gmail.com)



# SÉCURITÉ DES DONNÉES & BLOCKCHAIN



## OBJECTIFS

- ☐ Présenter les principes fondamentaux de la sécurité des données
- ☐ Découvrir les mécanismes de sécurité
- ☐ Savoir utiliser des mécanismes cryptographiques
- ☐ Présenter la technologie Blockchain
- ☐ Sécuriser les données à travers la Blockchain

# SÉCURITÉ DES DONNÉES & BLOCKCHAIN

Elément 1



Elément 2



## PLAN - SÉCURITÉ DES DONNÉES

- ☐ Introduction à la sécurité des données
- ☐ Menaces à la sécurité des données
- ☐ Principes de base de la sécurité des données
- ☐ Méthodes de protection des données
- ☐ Gestion des risques
- ☐ Normes et réglementations
- ☐ Bonnes pratiques en matière de sécurité des données
- ☐ Gestion des incidents de sécurité des données

## PLAN - BLOCKCHAIN

- ☐ Introduction à la Blockchain
- ☐ Fonctionnement de la Blockchain
- ☐ Types de Blockchain
- ☐ Applications de la Blockchain
- ☐ Sécurité et Confidentialité dans la Blockchain
- ☐ Limites et Défis de la Blockchain
- ☐ Cas d'études et Exemples concrets
- ☐ Tendances et Évolutions de la Blockchain
- ☐ Perspectives et Future de la Blockchain
- ☐ Cas Pratiques et Projets

## INTRODUCTION À LA SÉCURITÉ DES DONNÉES

1. DÉFINITION DE LA SÉCURITÉ DES DONNÉES
2. IMPORTANCE DE LA SÉCURITÉ DES DONNÉES
3. PRINCIPAUX OBJECTIFS DE LA SÉCURITÉ DES DONNÉES

## SÉCURITÉ DES DONNÉES - DÉFINITION

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



## SÉCURITÉ DES DONNÉES - IMPORTANCE

Aujourd'hui, les données digitales sont indispensables aux entreprises, et le marché du Big Data devrait peser 103 milliards de dollars d'ici 2027\*.

La sécurité des systèmes d'information est un défi permanent et il est essentiel de mettre en place des mesures de sécurité appropriées pour atténuer ces risques et protéger les informations sensibles

\* <https://www.talend.com>

## SÉCURITÉ DES DONNÉES — IMPORTANCE

Les pertes causées par des attaques informatiques sont au plus haut

Average Total Cost Per Data Breach, in USD Million, By Country or Region, Global, 2022

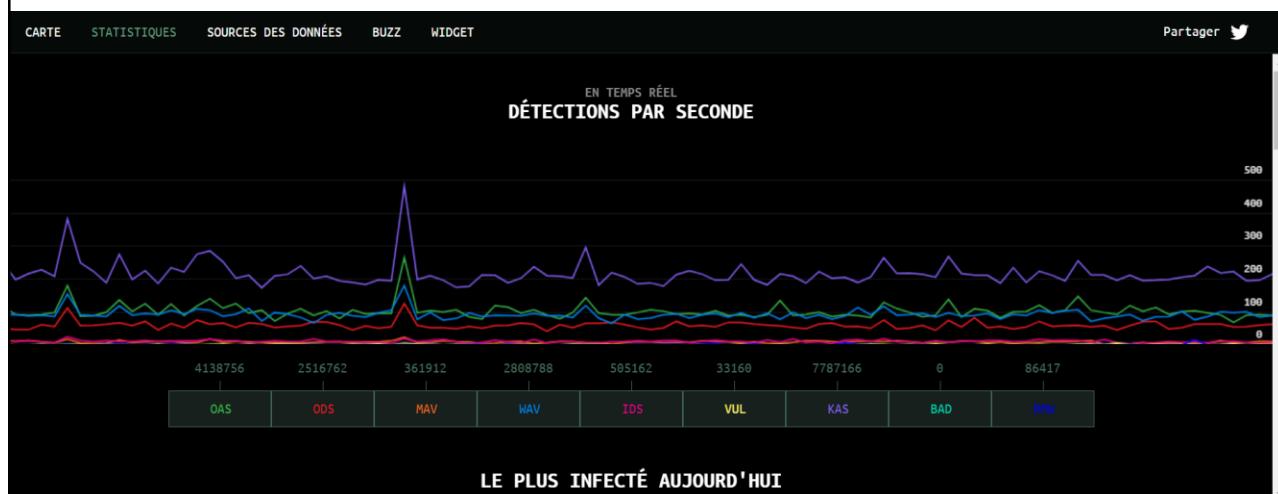


Source: Ponemon Institute, IBM

## SÉCURITÉ DES DONNÉES — IMPORTANCE

Statistiques des attaques en temps réel

<https://cybermap.kaspersky.com/>



## SÉCURITÉ DES DONNÉES - OBJECTIFS

- Protection des informations
- Aide à préserver la réputation (organisme, entreprise, ...)
- Avantages concurrentiels
- Réduction des coûts de support et de développement

## SÉCURITÉ DES DONNÉES — OBJECTIFS

### HYGIÈNE NUMÉRIQUE

- CONFIDENTIALITÉ DES DONNÉES
- INTÉGRITÉ DES DONNÉES
- DISPONIBILITÉ
- NON-RÉPUDIATION
- PRÉSERVATION DE LA RÉPUTATION

# SÉCURITÉ DES DONNÉES — OBJECTIFS

## CONFIDENTIALITÉ DES DONNÉES

Garder les données, stockées ou transmises, secrètes ou privées

→ CHIFFREMENT

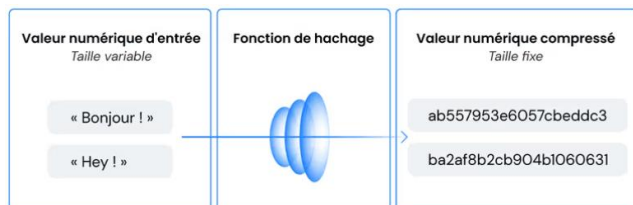


# SÉCURITÉ DES DONNÉES — OBJECTIFS

## INTÉGRITÉ

S'assurer que les données sont authentiques, exactes et fiables.

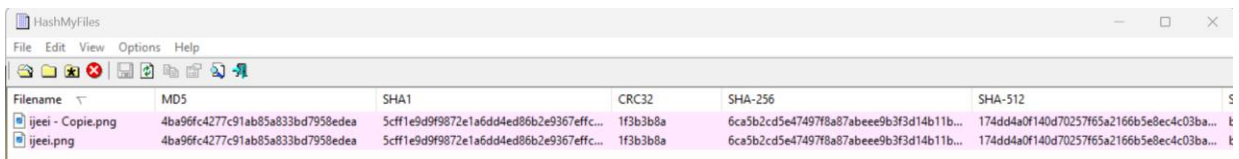
→ FONCTIONS DE HACHAGE : MD5, SHA1, SHA256



# SÉCURITÉ DES DONNÉES — OBJECTIFS

## INTÉGRITÉ

Exemple : HashMyFiles:



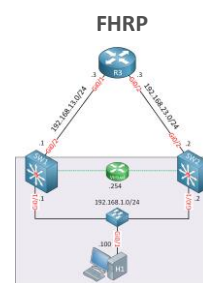
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512
ijeei - Copie.png	4ba96fc4277c91ab85a833bd7958edea	5cff1e9d9f9872e1a6dd4ed86b2e9367effc...	1f3b3b8a	6ca5b2cd5e47497f8a87abee9b3f3d14b11b...	174dd4a0f140d70257f65a2166b5e8ec4c03ba...
ijeei.png	4ba96fc4277c91ab85a833bd7958edea	5cff1e9d9f9872e1a6dd4ed86b2e9367effc...	1f3b3b8a	6ca5b2cd5e47497f8a87abee9b3f3d14b11b...	174dd4a0f140d70257f65a2166b5e8ec4c03ba...

# SÉCURITÉ DES DONNÉES — OBJECTIFS

## DISPONIBILITÉ

Assurer l'accès aux données à tout moment par les personnes autorisées

→ LA DUPLICATION, ...





# MENACES À LA SÉCURITÉ DES DONNÉES

1. MENACES INTERNES
2. MENACES EXTERNES

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### MENACE

Une situation critique qui porte atteinte à la sécurité d'un système suite à un événement nocif qu'il soit:

- ❖ **Accidentelle** (erreur humaine ou défaillance)
- ❖ **Naturelle** (catastrophes naturelles)
- ❖ **Intentionnelle** (attaques)

On distingue deux types de menaces :

- ☐ MENACES INTERNES
- ☐ MENACES EXTERNES

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

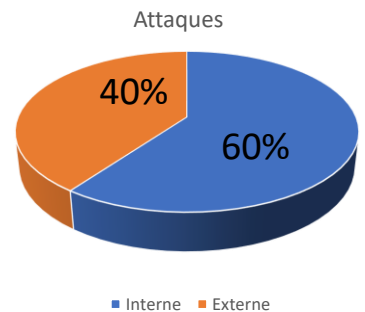
### ☐ MENACES INTERNES

- ❖ Une menace interne est un type de cyberattaque provenant d'une personne qui travaille pour une organisation ou qui a un accès autorisé à ses réseaux ou systèmes.

- ❖ 60% d'attaques viennent de l'intérieur :

Employé de l'entreprise

- Malveillant
  - Employé licencié
  - Administrateur mécontent
  - ...
- Négligeant



NB: Point faible des entreprises → manque de traçabilité

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ☐ MENACES INTERNES

La lutte contre les menaces internes

- ❖ Formation des employés et des utilisateurs
- ❖ Gestion des identités et des accès
- ❖ Implication de l'IA
  - ✓ Analyse du comportement des utilisateurs
  - ✓ Renforcer les stratégies de prévention
  - ✓ ...

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### MENACES EXTERNES

- ❖ Les menaces externes proviennent d'acteurs malveillants extérieurs à une organisation qui tentent d'obtenir un accès non autorisé aux réseaux, aux systèmes et aux données sensibles.
- ❖ En règle générale, ils utilisent les vulnérabilités du système pour obtenir un accès initial, puis se donnent des privilèges supplémentaires afin qu'ils puissent atteindre leurs objectifs.

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### MENACES EXTERNES

Les menaces de cybersécurité externes se répartissent en trois catégories de base :

- ☐ Logiciels malveillants, comme les ransomware
- ☐ Piratage, comme les attaques par déni de service distribué (DDoS)
- ☐ Ingénierie sociale, comme le phishing

# SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

## MENACES EXTERNES

- Les attaques par Malware
- Les attaques par Phishing
- Credential Stuffing
- Les attaques par déni de services (DDoS)
- Les attaques par force brutes
- Les vulnérabilités logicielles
- Les violations de données
- Les failles de sécurité physique
- Injection SQL

# SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

## ➤ Les attaques par Malware

Sont tout type de logiciel malveillant conçu pour causer des dommages à un ordinateur, un serveur, un client ou un réseau informatique et/ou une infrastructure à l'insu de l'utilisateur final.

La plupart des types de logiciels malveillants peuvent être classés dans l'une des catégories suivantes :



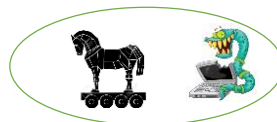
Virus



Ver



Cheval de Troie



Logiciels malveillants hybrides

Logiciels publicitaires



Ransomware

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ❑ Les attaques par Malware

Il existe différents types de malware :

- ✓ **Les Spiwares** : s'infiltrer et collectent des données et les transférer à son utilisateur
- ✓ **Le ransomware** : volent vos informations et proposent de vous les rendre en échange d'une somme d'argent
- ✓ **Le cheval de Troie** : un logiciel malveillant, souvent téléchargé par mégarde par l'utilisateur qui clique sur la pièce jointe d'un email piégé, qui a pour but de faire profiter à un tiers les ressources de votre ordinateur
- ✓ **Les vers** : ciblent les vulnérabilités des systèmes d'exploitation pour s'installer dans les réseaux. Plus faciles à programmer qu'un virus, ils utilisent internet sous toutes ses formes pour se propager via des emails, des sites web ou des serveurs FT

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Les attaques par Malware (suite)

- ✓ **Les virus** : Un virus est un morceau de code, un programme qui s'insère dans une application et s'exécute lorsque celle-ci est ouverte. Il a la particularité de s'auto-reproduire en infectant d'autres programmes
- ✓ **Les Rootkits** : sont des logiciels qui permettent au cybercriminel de contrôler à distance l'ordinateur d'une victime avec des privilèges administratifs complets
- ✓ **Les Botnets ou Bot** : Un bot est un logiciel qui exécute des tâches automatisées sur commande. Utilisés à des fins malveillantes, ils se propagent automatiquement et peuvent se reconnecter à un serveur central.  
Les bots sont utilisés en très grand nombre pour créer un botnet (un réseau de bots) pour lancer des attaques de grande envergure à distance comme les attaques DDoS.

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ DDoS (Denial of Service)

Les attaques DoS ou DDoS (denial of service attack – en français Dénier de Service) sont des attaques qui visent à paralyser un service et le rendre indisponible.

- ❖ **DoS (denial of service attack)** : Une attaque avec une seule source non distribuée
- ❖ **DDoS (distributed denial of service attack)** : L'attaquant utilise un réseau d'ordinateurs et objets internet sous son contrôle pour multiplier les sources et la force de l'attaque. Plusieurs différentes techniques sont possibles pour amplifier l'attaque

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Man in the Middle (MiTM)

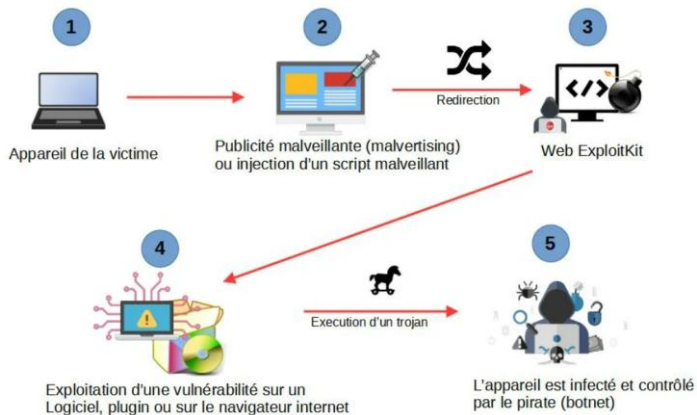
Un type de cyberattaque où les attaquants interceptent une communication réseau ou un transfert de données existant, soit en écoutant aux portes, soit en se faisant passer pour un participant légitime



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Drive-By Download

Désigne une cyberattaque dans laquelle un script malveillant provoque le téléchargement et l'installation d'un programme sur le périphérique d'un utilisateur, sans l'autorisation explicite de ce dernier.



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Phishing (ou hameçonnage)

- ✓ Sont l'un des types de cyberattaques les plus répandus. Il s'agit d'une attaque d'ingénierie sociale dans laquelle un attaquant se fait passer pour un contact de confiance et envoie à la victime de faux courriers électroniques
- ✓ Sans s'en rendre compte, la victime ouvre le courrier et clique sur le lien malveillant ou ouvre la pièce jointe du courrier. Ce faisant, les attaquants accèdent à des informations confidentielles et à des identifiants de compte. Ils peuvent également installer des logiciels malveillants par le biais d'une attaque de phishing.

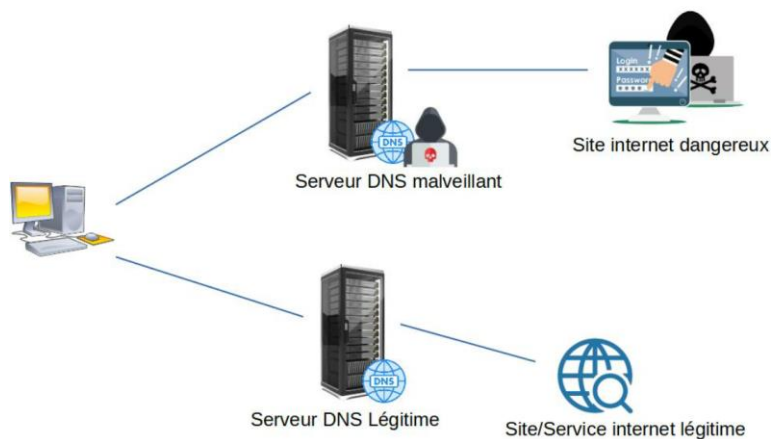
## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ DNS Spoofing / Hijack DNS

- ✓ Le pirate modifie les serveurs DNS afin d'envoyer le trafic vers un faux site web ou site "usurpé".
- ✓ Une fois sur le site frauduleux, la victime peut saisir des informations sensibles qui peuvent être utilisées ou vendues par le pirate.
- ✓ Le pirate peut également construire un site de mauvaise qualité avec un contenu désobligeant ou incendiaire pour donner une mauvaise image d'une entreprise concurrente.

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ DNS Spoofing / Hijack DNS





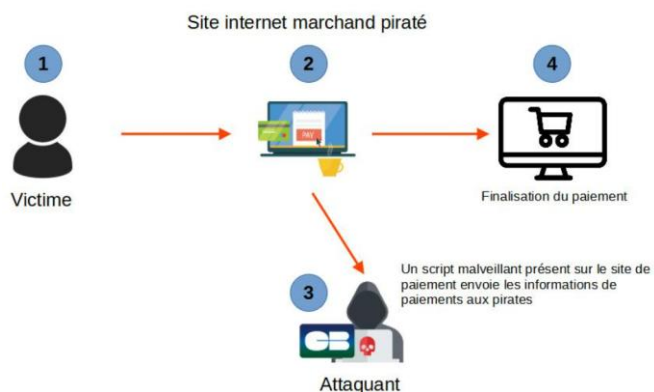
## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Shopping Skimming

- ✓ Consiste à voler les données bancaires.
- ✓ Parmi les nombreuses techniques utilisées, on trouve, celle du piratage des sites marchands.
- ✓ Les pirates injecte un script malveillant qui récupère les données bancaires au moment du paiement.
- ✓ Cette attaque est sournoise car tout est invisible, sauf si votre antivirus détecte le script malveillant ou la connexion vers le serveur du pirate.

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Shopping Skimming



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Brute force (Brute force Attack)

- ✓ Utilise une approche par des essais en continue pour deviner les informations de connexion, les informations d'identification, un hash et les clés de chiffrement.
- ✓ L'attaquant soumet des combinaisons de noms d'utilisateur et de mots de passe jusqu'à trouver la bonne combinaison.



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Cross-Site Scripting (XSS)

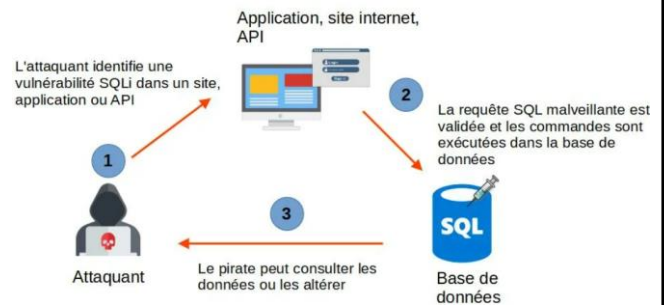
- ✓ Un type d'injection, dans lequel des scripts malveillants sont injectés dans des sites web par ailleurs bénins et de confiance.
- ✓ Les attaques XSS se produisent lorsqu'un attaquant utilise une application web pour envoyer un code malveillant, généralement sous la forme d'un script côté navigateur, à un autre utilisateur final.
- ✓ Les failles qui permettent à ces attaques de réussir sont assez répandues et se produisent partout où une application web utilise les entrées d'un utilisateur dans la sortie qu'elle génère sans les valider ou les coder.



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ SQL Injection (SQLi)

- ✓ Une vulnérabilité de sécurité web qui permet à un attaquant d'interférer avec les requêtes qu'une application effectue dans sa base de données.
- ✓ Elle permet généralement à un attaquant de visualiser des données qu'il n'est normalement pas en mesure de récupérer.



## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

### ➤ Cryptojacking

- ✓ Consiste à faire miner de la monnaie virtuelle en utilisant la puissance de calcul de l'appareil à l'insu de l'utilisateur.
- ✓ Cette cyberattaque peut prendre essentiellement trois formes :
  - Un Trojan Miner qui opère sur la machine et mine de la monnaie en utilisant le CPU ou GPU
  - Une extension malveillante sur le navigateur internet qui mine
  - Un site interne qui charge un JavaScript pour faire miner les visiteurs

## SÉCURITÉ DES DONNÉES — PRINCIPAUX MENACES

Avec l'arrivée de l'IA on voit émerger de nouvelles arnaques comme:

- **Smishing** : cible les individus par SMS (Short Message Service) ou messages texte. Le terme est une combinaison de « SMS » et de « phishing ».
- **Vishing** (hameçonnage vocal): Appels vocaux (via téléphone traditionnel ou services VoIP)
- **Deep fakes** : permet notamment la superposition de fichiers audios et/ou vidéos sur d'autres fichiers de manière à créer de faux contenus

## CHAPITRE 3 : PRINCIPES DE BASE DE LA SÉCURITÉ DES DONNÉES



## SÉCURITÉ DES DONNÉES — PRINCIPES

### Triade CIA

Proposé à partir de 1989 exprime les trois principales propriétés à garantir

- ❖ **Confidentialité** : garantit que les informations sensibles ne sont accessibles qu'aux personnes autorisées.
- ❖ **Intégrité** : se concentre sur le maintien de l'exactitude et de la cohérence des données, en veillant à ce qu'elles ne soient pas altérées pendant le stockage ou la transmission
- ❖ **Disponibilité** : garantit que les utilisateurs autorisés peuvent accéder aux données à tout moment

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### LE PROTOCOLE TRIPLE A

Ce modèle d'intéresse davantage aux étapes de contrôle d'accès.

- ☐ **Authentification** : qui veut accéder ? une preuve de l'identité (suit l'**identification**).
- ☐ **Autorisation** : a-t-il le droit d'effectuer les actions demandées ?
- ☐ **Accounting/Audit** : Quelles sont les opérations qui ont été effectuées par l'utilisateur.

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### PENTAGONE DE CONFIANCE

Le modèle défini par PAISIELLO en 2006. Il précise la confiance que peut avoir un utilisateur vis-à-vis d'un SI.

1. **Confidentialité** – Protection des données contre tout accès non autorisé.
2. **Intégrité** – Garantie que les données ne sont pas modifiées de manière non autorisée.
3. **Disponibilité** – Assurance que le système et les données restent accessibles en permanence.
4. **Authentification** – Vérification de l'identité des utilisateurs et des entités.
5. **Traçabilité** – Capacité à enregistrer et suivre les actions effectuées dans le système.

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### Critères de sécurité selon la norme ISO 27001

- ☐ Confidentialité – protéger les informations sensibles.
- ☐ Intégrité – garantir l'exactitude et la fiabilité des données.
- ☐ Disponibilité – Assurer l'accès permanent aux informations.
- ☐ Traçabilité – Suivre et identifier les accès aux données.

# SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

## OBJECTIFS DE SÉCURITÉ RECHERCHÉS

- ❑ **Confidentialité** : L'information ne doit pas divulguée qu'à des utilisateurs autorisés
- ❑ **Intégrité** : L'information ne doit être modifiée que par utilisateurs autorisés
- ❑ **Disponibilité** : L'information et les services doivent être accessibles au moment souhaité
- ❑ **Authentification** : Prouver l'identité d'un utilisateur ou d'un service
- ❑ **Autorisation** : Contrôler l'accès à l'information et/ou aux services
- ❑ **Non répudiation** : Ne pas nier l'origine du message
- ❑ **Audit** : Détecter les défaillances et les corriger, suivre les failles

# SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

## CONFIDENTIALITÉ

Assurer la **Confidentialité** consiste à rendre les données sensibles inintelligibles aux personnes/services non autorisés.

### Exemple

- ❑ Les mots de passe
- ❑ Données médicales
- ❑ Courrier électronique

### Type d'accès

- ❑ Lecture directe
- ❑ Impression des documents
- ❑ Détection de l'existence d'une donnée
- ❑ Requêtes utilisées par l'utilisateur

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### INTÉGRITÉ

L'**intégrité** est une propriété qui permet de vérifier que les données n'ont pas été modifiées ou détruites, que ça soit de façon accidentelle ou malveillante.

#### Exemple :

- ☐ Transactions financières
- ☐ Programmes et logiciels
- ☐ Communications

#### Type d'accès :

- ☐ Ecriture
- ☐ Modification du contenu ou métadonnées
- ☐ Création de nouvelles données

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### DISPONIBILITÉ

La propriété de **disponibilité** consiste à assurer l'accès à une quelconque ressource (services ou données) autorisée à l'endroit et au moment prévu.

#### Exemple :

- ☐ Disponibilité d'un serveur ou d'une ressource matérielle

#### Garantir également :

- ☐ Un temps de réponse acceptable
- ☐ Allocation des ressources équitables
- ☐ L'accès au services



## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### AUTHENTIFICATION

Vérifier la prétendue identité d'un utilisateur, d'un programme ou d'une machine.

L'authentification est une étape qui précède le contrôle d'accès.

#### Fonctionnalités associées :

- ☐ Gestion des identités : création , modification, suppression, etc.
- ☐ Protection des informations d'authentification (**credentials**)
- ☐ Exploitation des systèmes d'authentification unique (**single sign on**)
- ☐ Renforcement par authentification à plusieurs facteurs (**strong authentication**)

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### AUTORISATION

Implique les principes de contrôle d'accès et de gestion des droits. Elle regroupe les modèles et fonctions qui gèrent l'accès aux ressources selon des politiques et des règles bien définies.

#### Fonctionnalités associées :

- ☐ Formaliser et mettre à jour les règles et droits d'accès.
- ☐ Administrer le système : octroi, suppression et vérification des droits
- ☐ Gérer les mise à jour et les conflits possibles entre différentes règles ou politiques.

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### NON RÉPUDIATION

- Fournit la preuve indéniable qu'une action a bien été effectuée.
- Utilisée dans les transactions et la certifications des documents.
- Se base sur les signatures digitales.

#### Exemple :

- ☐ Achat en ligne
- ☐ Contrat électronique

#### Aspects :

- ☐ Preuve **d'origine** : la personne ne peut nier être la source de l'action.
- ☐ Preuve de **réception** : le destinataire ne peut nier la réception d'un document ou d'un ordre.

## SÉCURITÉ DES DONNÉES — PROPRIÉTÉS

### AUDITABILITÉ

Permet de détecter, retracer et enregistrer tous les événements qui surviennent dans un système.

#### Exemple :

- ☐ Tentatives d'attaques
- ☐ Accès non autorisé
- ☐ Mot de passe erroné
- ☐ Opération non conforme au procédures internes

- ☐ **Auditabilité** : maîtrise complète et permanente sur le système pendant d'une certaine période.
- ☐ **Audit** : enregistrement complet et suffisant de tous les événements normaux ou anormaux pour une analyse ultérieure.