

**COLLEGE LA PREVOYANCE DE MAKEPE MISSOKE****DEPARTEMENT D'INFORMATIQUE****DEVOIR SURVEILLÉ N°1****ANNEE SCOLAIRE : 2025 – 2026****MATIERE : INFORMATIQUE****DUREE : 1H30****COEFFICIENT : 2****CLASSE : 1^{ère} A4****Compétences visées :**

- Enoncer les principes fondamentaux de la sécurité informatique
- Décrire quelques techniques de protection des données
- Décrire quelques moyens de sécurité de son espace de travail

EPREUVE THEORIQUE D'INFORMATIQUE**I/ ENVIRONNEMENT NUMERIQUE ET SECURITE INFORMATIQUE****Exercice 1 : Sécurité informatique**

M. TENE est le responsable de la sécurité informatique dans une PME (Petite et Moyen Entreprise). Il met en place les mesures suivantes afin de renforcer la sécurité au sein de la PME :

- la protection des fichiers sensibles en écriture (Mesure 1),
- les sauvegardes journalières de nouvelles données sensibles de l'entreprise sur le Cloud (Mesure 2),
- le conditionnement de l'accès à la salle des serveurs par la lecture des empreintes digitales (Mesure 3).

- 1.1. Définir : sécurité informatique, système de sécurité **2pts**
- 1.2. Présenter deux avantages de la sécurité informatique. **1pt**
- 1.3. Nommer puis expliquer chacun des trois principes fondamentaux de sécurité informatique mis en œuvre à travers les mesures de M TENE **3pts**
- 1.4. Donner le schéma représentant les principes de la sécurité informatique **1pt**
- 1.5. Hormis de la triade CIA, citer deux autres principes complémentaire de la sécurité informatique **1pt**

Exercice 2 : Protection des données

Votre oncle TCHOKOTE qui est professeur d'informatique a écrit un bord d'informatique de la classe de 1^{ère} A4. Il a donc sauvegardé le fichier numérique sur son ordinateur. A son absence, l'un de ses collègues a pu accéder à son ordinateur, il prit donc ce fichier et se mit à imprimer le document pour les vendre. Etant au courant, votre oncle menace son collègue de porter plainte.

- 2.1. Qu'aurait fait votre oncle pour éviter l'accès à ses données ? **1pt**
- 2.2. Donner 04 techniques de protection qu'il pourra utiliser **2pt**
- 2.3. Expliquer en quoi consiste la cryptographie **1pt**
- 2.4. Un de ses amis lui demande de compresser les données de son ordinateur. Pensez-vous que la compression soit une méthode de sécurité appropriée pour ce cas ? **1pt**

Exercice 3 : Sécurité de son espace de travail

A) Lors d'un TP en salle informatique du collège, votre camarade ouvre une des machines dans l'intention d'installer un jeu vidéo. Cependant elle est bloquée par un mot de passe Administrateur.

- A.3.1. Définir Mot de passe, antivirus **2pts**
- A.3.2. Quel type de compte a ouvert votre camarade **1pt**
- A.3.3. Enumérer les autres types de compte sous Windows que vous connaissez **1pt**

B) La salle informatique étant connecté sur internet votre camarade veut envoyer un message chiffré.

- B.3.1. Définir Chiffrement **1pt**
- B.3.2. Comment appelle-t-on le résultat du chiffrement **1pt**
- B.3.3. Distinguer l'authentification et l'identification d'un utilisateur **1pt**

*"Aucun Fugitif n'a jamais débordé les limites de la terre!
Où que vous soyez, l'Informatique vous rattrapera !!! "*

Correction de l'épreuve théorique d'informatique

Classe : 1ère A4 – DSN°1 – Octobre 2025

I/ ENVIRONNEMENT NUMÉRIQUE ET SÉCURITÉ INFORMATIQUE

Exercice 1 : Sécurité informatique

1.1. Définir : sécurité informatique, système de sécurité

- **Sécurité informatique** : Ensemble des moyens techniques, organisationnels, juridiques et humains mis en œuvre pour protéger les systèmes d'information contre les menaces, les intrusions et les accidents, afin de garantir la confidentialité, l'intégrité et la disponibilité des données.
- **Système de sécurité** : Ensemble des dispositifs (matériels, logiciels, procédures) destinés à assurer la protection d'un système d'information contre les accès non autorisés, les modifications, les vols ou les destructions.

1.2. Présenter deux avantages de la sécurité informatique

- Protection des données sensibles contre les accès non autorisés et les fuites d'informations.
- Continuité de service et disponibilité des données en cas de sinistre grâce aux sauvegardes.

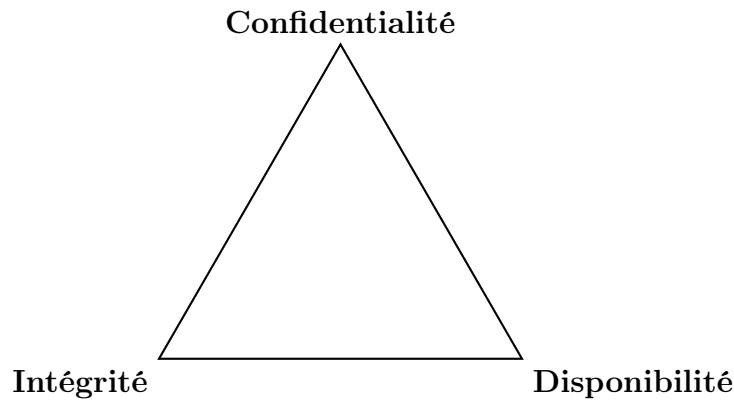
Autres réponses possibles : conformité légale, confiance des clients, etc.

1.3. Nommer puis expliquer chacun des trois principes fondamentaux de sécurité informatique mis en œuvre à travers les mesures de M. TENE

Les trois principes fondamentaux sont la **Confidentialité**, l'**Intégrité** et la **Disponibilité** (triade CIA).

- **Mesure 1 : protection des fichiers sensibles en écriture** → garantit l'**Intégrité** : les fichiers ne peuvent pas être modifiés sans autorisation.
- **Mesure 2 : sauvegardes journalières sur le Cloud** → garantit la **Disponibilité** : en cas de perte ou de destruction, les données peuvent être restaurées.
- **Mesure 3 : accès à la salle des serveurs par empreintes digitales** → garantit la **Confidentialité** : seules les personnes autorisées peuvent accéder aux serveurs.

1.4. Donner le schéma représentant les principes de la sécurité informatique



1.5. Hormis de la triade CIA, citer deux autres principes complémentaires de la sécurité informatique

- **Authentification** (vérification de l'identité)
- **Non-répudiation** (impossibilité de nier une action)

Autres : traçabilité, contrôle d'accès, etc.

Exercice 2 : Protection des données

2.1. Qu'aurait fait votre oncle pour éviter l'accès à ses données ?

Il aurait dû :

- Verrouiller sa session lorsqu'il quitte son ordinateur.
- Protéger son compte par un mot de passe fort.
- Chiffrer le fichier contenant le bord d'informatique.
- Restreindre les droits d'accès au fichier.

2.2. Donner 04 techniques de protection qu'il pourra utiliser

1. Le chiffrement des données.
2. La gestion des droits d'accès (permissions).
3. L'authentification forte (mot de passe complexe, biométrie).
4. Les sauvegardes régulières sur un support sécurisé.

2.3. Expliquer en quoi consiste la cryptographie

La cryptographie est la science et technique qui consiste à transformer un message clair en un message chiffré (inintelligible) à l'aide d'une clé, afin de garantir la confidentialité, l'intégrité et l'authenticité des données lors de leur stockage ou de leur transmission. Seul le destinataire possédant la clé de déchiffrement peut lire le message.

2.4. Un de ses amis lui demande de compresser les données de son ordinateur. Pensez-vous que la compression soit une méthode de sécurité appropriée pour ce cas ?

Non. La compression réduit la taille des données mais ne les protège pas. Un fichier compressé peut être décompressé par n'importe qui. Ce n'est donc pas une méthode de sécurité. Pour sécuriser les données, il faut les chiffrer.

Exercice 3 : Sécurité de son espace de travail

A) Compte et mot de passe

A.3.1. Définir Mot de passe, antivirus

- **Mot de passe** : Chaîne de caractères secrète utilisée pour authentifier un utilisateur et contrôler l'accès à une ressource (compte, fichier, réseau).
- **Antivirus** : Logiciel destiné à détecter, bloquer et supprimer les logiciels malveillants (virus, vers, chevaux de Troie, etc.) sur un ordinateur.

A.3.2. Quel type de compte a ouvert votre camarade ?

Elle a ouvert un **compte utilisateur standard** (ou limité), car elle est bloquée par le mot de passe Administrateur lorsqu'elle tente d'installer un jeu.

A.3.3. Enumérer les autres types de compte sous Windows que vous connaissez

- Compte Administrateur
- Compte Utilisateur standard
- Compte Invité
- Compte Microsoft
- Compte local

B) Chiffrement

B.3.1. Définir Chiffrement

Le chiffrement est le procédé qui consiste à transformer un message clair en un message inintelligible (chiffré) à l'aide d'un algorithme et d'une clé, afin d'en garantir la confidentialité.

B.3.2. Comment appelle-t-on le résultat du chiffrement ?

Le résultat du chiffrement s'appelle le **cryptogramme** ou **message chiffré**.

B.3.3. Distinguer l'authentification et l'identification d'un utilisateur

- **Identification** : L'utilisateur déclare son identité (par exemple, saisir son nom d'utilisateur). C'est le fait de se nommer.
- **Authentification** : L'utilisateur prouve son identité (par exemple, mot de passe, empreinte digitale). C'est la vérification de l'identité déclarée.