1. Quelle est la définition de la triade CID en sécurité de l'information ?

A. Confidentialité, Intégrité, Disponibilité

B. Conformité, Intégrité, Durabilité

C. Confidentialité, Identification, Disponibilité

2. Laquelle des options suivantes décrit correctement la "Confidentialité" dans la triade CID ?

A. Assurer que l'information est accessible uniquement aux personnes autorisées

B. Garantir que l'information est exacte et complète

C. Assurer que l'information est disponible quand on en a besoin

3. Quel aspect de la triade CID est principalement concerné par les attaques par déni de service (DoS) ?

A. Confidentialité

B. Intégrité

C. Disponibilité

4. Parmi les actions suivantes, laquelle contribue principalement à l'Intégrité dans la triade CID ?

A. Utiliser le cryptage pour protéger les données

B. Mettre en place des contrôles d'accès

C. Utiliser des sommes de contrôle (checksums) et des signatures numériques

5. Que signifie la "Disponibilité" dans le cadre de la triade CID ?

A. Protéger les données contre les accès non autorisés

B. Assurer que les systèmes et les données sont disponibles pour les utilisateurs autorisés en temps voulu

C. Maintenir l'exactitude et la fiabilité des données

6. Quelle méthode contribue principalement à la "Confidentialité" des données ?

A. Redondance des serveurs

B. Chiffrement des données

C. Contrôle des versions des fichiers

7. Quel concept est central pour maintenir l'Intégrité des données ?

A. Accès en lecture seule

B. Redondance des systèmes

C. Utilisation de protocoles de chiffrement

8. Quelle situation illustre une violation de la Disponibilité ?

A. Un employé non autorisé accède aux données sensibles

B. Un fichier est accidentellement modifié

C. Un serveur critique est hors ligne pendant plusieurs heures

9. Quel est le principal objectif des contrôles d'accès dans le contexte de la triade CID ?

A. Prévenir la perte de données

B. Assurer que seules les personnes autorisées peuvent accéder à certaines informations

C. Garantir la disponibilité des ressources

10. Quelle pratique est essentielle pour assurer la Disponibilité des systèmes ?

A. Mise en œuvre de politiques de sauvegarde régulières

B. Utilisation de protocoles de chiffrement forts

C. Surveillance et mise à jour régulière des systèmes de détection d'intrusion

11. Comment la triade CID s'applique-t-elle à la gestion des mots de passe ?

A. Utilisation de mots de passe complexes pour la Confidentialité

B. Changement fréquent des mots de passe pour l'Intégrité

C. Sauvegarde régulière des mots de passe pour la Disponibilité

12. Qu'est-ce qui pourrait le plus compromettre l'Intégrité des données dans une base de données ?

A. L'absence de sauvegarde régulière

B. Une attaque par injection SQL

C. Un accès non autorisé aux fichiers

13. La mise en place de pare-feux contribue principalement à quel aspect de la triade CID ?

A. Confidentialité

B. Intégrité

C. Disponibilité

14. Quel exemple représente une mesure visant à assurer la Confidentialité ?

A. Utilisation de RAID pour la tolérance aux pannes

B. Utilisation de VPN pour protéger les communications

C. Utilisation de logs d'audit pour surveiller les modifications

15. Pourquoi est-il important d'avoir une stratégie de récupération après sinistre pour la Disponibilité ?

A. Pour protéger les données contre les accès non autorisés

B. Pour garantir que les données peuvent être restaurées en cas de perte ou de panne

C. Pour maintenir l'exactitude des données pendant les opérations de récupération

16. Une entreprise de commerce électronique constate que son site web est souvent hors ligne en raison d'attaques par déni de service (DoS). Quelle partie de la triade CID est affectée et quelle mesure de sécurité devrait-elle mettre en place pour résoudre ce problème ?

A. Confidentialité ; Chiffrement des données

B. Intégrité ; Utilisation de sommes de contrôle

C. Disponibilité ; Mise en place de solutions de prévention des DoS

17. Un hôpital découvre qu'un employé non autorisé a accédé aux dossiers médicaux des patients. Quel aspect de la triade CID a été compromis et quelle solution pourrait être mise en œuvre pour éviter ce problème à l'avenir ?

A. Disponibilité ; Sauvegarde régulière des données

B. Intégrité ; Utilisation de signatures numériques

C. Confidentialité ; Mise en œuvre de contrôles d'accès stricts

18. Une société financière remarque que certains de ses fichiers critiques ont été modifiés de manière inattendue. Quel élément de la triade CID est en jeu et quelle mesure devrait-elle adopter pour protéger ses données ?

A. Disponibilité ; Installation de systèmes de sauvegarde

B. Confidentialité ; Utilisation de VPN

C. Intégrité ; Mise en place de contrôles de version et de logs d'audit

19. Une petite entreprise de technologie subit une perte de données suite à une panne matérielle. Quel aspect de la triade CID est impacté et quelle solution peut aider à prévenir ce problème à l'avenir ?

A. Confidentialité ; Utilisation de mots de passe forts

B. Intégrité ; Contrôle d'accès en lecture seule

C. Disponibilité ; Mise en œuvre de sauvegardes régulières et de systèmes de redondance

20. Une entreprise de médias sociaux veut s'assurer que seules les personnes autorisées peuvent voir les informations privées de ses utilisateurs. Quel aspect de la triade CID cela concerne-t-il et quelle mesure pourrait-elle prendre ?

A. Intégrité ; Utilisation de sommes de contrôle

B. Disponibilité ; Mise en place de serveurs redondants

C. Confidentialité ; Chiffrement des données et mise en œuvre de politiques de contrôle d'accès

21. Une organisation gouvernementale découvre qu'un attaquant a falsifié certaines données sensibles. Quel élément de la triade CID a été compromis et quelle action devrait être entreprise pour renforcer la sécurité ?

A. Disponibilité ; Surveillance des systèmes

B. Intégrité ; Utilisation de signatures numériques et de logs d'audit

C. Confidentialité ; Utilisation de chiffrement fort

22. Une entreprise de logiciels s'inquiète de la possibilité que ses données ne soient pas disponibles pendant une catastrophe naturelle. Quel aspect de la triade CID est concerné et quelle mesure préventive pourrait être mise en place ?

A. Confidentialité ; Mise en œuvre de VPN

B. Intégrité ; Utilisation de protocoles de vérification

C. Disponibilité ; Élaboration d'un plan de reprise après sinistre

23. Une banque en ligne remarque que les connexions à son système sont très lentes et parfois indisponibles. Quel aspect de la triade CID est touché et quelle solution devrait être mise en œuvre ?

A. Confidentialité ; Utilisation de chiffrement SSL

B. Intégrité ; Mise en place de checksums

C. Disponibilité ; Mise en place de solutions de mise en cache et de répartition de charge

24. Une université veut s'assurer que les notes des étudiants ne peuvent pas être modifiées sans autorisation. Quel aspect de la triade CID est en jeu et quelle mesure devrait-elle adopter ?

A. Confidentialité ; Utilisation de mots de passe forts

B. Intégrité ; Utilisation de contrôles de version et de permissions d'accès strictes

C. Disponibilité ; Mise en place de sauvegardes régulières

25. Une entreprise de développement de logiciels veut garantir que ses services en ligne sont toujours accessibles, même en cas de panne serveur. Quel aspect de la triade CID cela concerne-t-il et quelle solution pourrait-elle utiliser ?

A. Intégrité ; Utilisation de protocoles de chiffrement

B. Confidentialité ; Mise en œuvre de VPN

C. Disponibilité ; Utilisation de serveurs redondants et de solutions de répartition de charge