UNIVERSITE DE BISKRA 26/06/2019

GENIE ELECTRIQUE

RES&TELEC

LICENCE (SECURITE DE L'INFORMATION)

 Répondre par oui, non, néant EXAMEN 1h30mn 2019

Q1. La sécurité de l'information n'assure pas son intégrité ....................

Q2. L’intégrité de l'information assure que son état demeure intacte..................

Q3. La confidentialité des données est le maintien du secret des informations.............

Q4. La confidentialité : l’information n’est pas compréhensible par des personnes non

 autorisées........................

Q5. Parmi les critères de sécurité suivants, lequel n’est pas adapté à un système d’information

 A) Confidentialité B) Intégrité C) Insolvabilité D) Non-répudiation

**Q6.** La sécurité ne doit pas être perçue comme un frein à la bonne marche de l’organisation

 doit constituer un levier de réalisation de ses objectifs tels que spécifiés dans la stratégie

 générale.

 Une sécurité de l’information cohérente ne constitue pas un avantage compétitif.............

Q7. Parmi les propositions suivantes quelle est celle qui correspond le mieux au besoin de

 gérer la sécurité ?

 A) Traiter la sécurité comme une exigence du business............

 B) Appréhender et traiter la sécurité comme un processus continu.............

 C) Appréhender et traiter la sécurité comme un processus discontinu........

 D) Appréhender et traiter la sécurité comme un processus connu...............

Q8.La méthode cryptographique { Ck: Z/26Z→Z/26Z ; x→x+k mod 26} est dite de

 Lyapunov...............

Q9.Le nombre de clé de la méthode cryptographique de César est fixé à 26..............

Q10. La méthode cryptographique du carré de Polybe est difficilement cassable à cause de la

 nature de la base de caractère utilisé.....................

Q11. La méthode cryptographique de Vigenère est facilement cassable par méthode

 statistique..............

Q12.La méthode cryptographe de César est symétrique ....................

Q13.La méthode cryptographe de Vigenère est asymétrique........................

Q14. La méthode cryptographe RSA est asymétrique.....................

Q15. La clé des méthodes symétriques risque d'être piratée du fait qu'elle n'est pas envoyée

 par internet.............

Q16. La méthode RSA utilise une seule clé pour le chiffrement et le déchiffrement...........

Q17. la Méthode cryptographique de D.H est dite symétrique.........................

Q19.Les risques humain: la maladresse,l'inconscience la malveillance et l'ignorance

 détériore la sécurité de l'information et améliore celle du réseau informatique............

Q20.Les programmes malveillants: le virus, le ver, le cheval de Troie, la porte dérobée et le

 logiciel espion permettent une immunité plus forte aux attaques................

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 QUELQUE EXERCICES S\_INF

 **Exercice 1**

Définir la notion d'intégrité des données ainsi que les objectifs du contrôle d'intégrité.

**Réponse**

L’intégrité est l’état d’une chose qui est demeurée intacte. Pour ce qui concerne des données, l’objectif du contrôle d’intégrité est de vérifier qu’elles n’ont pas été altérées tant de façon intentionnelle qu’accidentelle.

**Exercice 2**

Quelles relations existent entre les critères d’intégrité et de confidentialité ?

**Réponse**

La confidentialité des données est le maintien du secret des informations. L’information n’a pas été modifiée de manière non autorisée (intégrité), l’information n’est pas compréhensible par des personnes non autorisées (confidentialité).

Les critères d’intégrité et de confidentialité sont complémentaires, lorsqu’ils sont réalisés par des fonctions *ad hoc* de sécurité, ils permettent de développer la confiance dans la véracité de l’information.

**Exercice 3**

Dans quelle mesure la notion de qualité des données est-elle liée à celle de sécurité ?

**Réponse**

La qualité est généralement une caractéristique d’excellence, reflétant une valeur, une compétence. Dans la mesure où des données possèdent un certain degré de sécurité et satisfont des exigences de disponibilité, d’intégrité ou de confidentialité, elles possèdent un degré intrinsèque de qualité et elles permettent d’offrir des services de qualité.

En respectant les critères de sécurité, la satisfaction d’exigences de la qualité comme la justesse et la fiabilité, peuvent être réalisées.

**exercice 4**

Parmi les critères de sécurité suivants, lequel n’est pas adapté à un système d’information ?

A) Confidentialité B) Intégrité C) Insolvabilité D) Non-répudiation

**Réponse :** C

**Exercice 5**

Dans quelle mesure peut-on considérer des principes d’éthique comme faisant partie d’une démarche de sécurité informatique ?

**Réponse**

Le dictionnaire nous rappelle que « *l’éthique est la science de la morale, l’art de diriger la conduite* ». Les qualités morales des acteurs qui conçoivent, gèrent, mettent en place, utilisent les systèmes informatiques sont nécessaires pour assurer les critères techniques de sécurité. On ne peut assurer l’intégrité ou la confidentialité des données par exemple, si les personnes qui sont habilitées à les manipuler ne sont pas intègres ou sont malveillantes. L’humain est toujours le maillon faible de la chaîne sécuritaire mais il peut être également producteur de sécurité à condition qu’il respecte une certaine éthique compatible avec les valeurs de sécurité de l’environnement dans lequel il opère.

**Exercice 6**

Sur quels principes se fonde la réalisation d’attaques informatiques ?

**Réponse**

La réalisation d’attaques informatiques se fonde sur le leurre, le détournement, l’usage abusif des technologies, la manipulation d’information, l’exploitation des failles et vulnérabilités, l’usurpation d’identité et de paramètres de connexion d’ayants droit.

**Exercice 7**

Quelle est la place de la maîtrise de la cybercriminalité dans une démarche de cybersécurité ?

**Réponse**

Il est nécessaire de renforcer la cybersécurité pour diminuer les vulnérabilités des environnements à protéger contre des cyberattaques, pour diminuer les opportunités de réaliser des malveillances, pour dissuader les attaquants potentiels.