

**Exercice 01 :** Questions à Choix Multiple

- |  |   |
|--|---|
| <ol style="list-style-type: none"> <li>1. .... signifie que les informations contenues dans un système informatique ne sont accessibles en lecture que par les personnes autorisées.             <ol style="list-style-type: none"> <li>a. Authentification</li> <li>b. Confidentialité</li> <li>c. Intégrité</li> <li>d. Disponibilité</li> </ol> </li> <li>2. .... signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées.             <ol style="list-style-type: none"> <li>a. Authentification</li> <li>b. Confidentialité</li> <li>c. Intégrité</li> <li>d. Disponibilité</li> </ol> </li> <li>3. Parmi les attaques ci-après, lesquelles vise la disponibilité:             <ol style="list-style-type: none"> <li>a. Usurpation d'identité</li> <li>b. Déné de service</li> <li>c. Modification du journal</li> <li>d. Bombardement et saturation du réseau</li> </ol> </li> <li>4. Le rôle de la sécurité en entreprise est de :             <ol style="list-style-type: none"> <li>a. Réduire les risques à niveau acceptable</li> <li>b. Prévenir tout risque</li> <li>c. Empêcher les utilisateurs de travailler librement</li> <li>d. Surveiller le bon fonctionnement des systèmes</li> </ol> </li> <li>5. L'une des importantes vulnérabilités dans le SI d'entreprises :             <ol style="list-style-type: none"> <li>a. L'inexpérience et risque lié aux utilisateurs</li> <li>b. La présence de ports USB sur les PCs</li> <li>c. L'utilisation des mots de passe au lieu de méthodes plus sûres</li> <li>d. Les connexions à réseau local</li> </ol> </li> <li>6. Un risque:             <ol style="list-style-type: none"> <li>a. est un danger éventuel plus ou moins prévisible.</li> <li>b. se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation.</li> <li>c. est l'ensemble des actions réalisées en prévention de la menace.</li> </ol> </li> </ol> | <ol style="list-style-type: none"> <li>7. Quelle procédé permettant d'assurer l'intégrité des données?             <ol style="list-style-type: none"> <li>a. Chiffrement symétrique</li> <li>b. Chiffrement asymétrique</li> <li>c. Fonction de hachage</li> <li>d. Certificat numérique</li> </ol> </li> <li>8. Quelle est la meilleure manière pour protéger l'information confidentielle ?             <ol style="list-style-type: none"> <li>a. Un bon anti-virus sur mon ordinateur.</li> <li>b. Un bon système de chiffrement du disque dur de mon ordinateur.</li> <li>c. Un pare-feu (firewall) efficace et surtout bien configuré sur mon ordinateur.</li> <li>d. Aucune des techniques ci-dessus ne répond totalement au besoin.</li> </ol> </li> <li>9. Parmi les propositions suivantes, laquelle ne concerne pas par les aspects techniques de la sécurité:             <ol style="list-style-type: none"> <li>a. Vol de matériel informatique</li> <li>b. Détection de l'intrusion</li> <li>c. Plan de sauvegarde</li> <li>d. Licence de logiciel</li> </ol> </li> <li>10. La sécurité de l'exploitation traite les points suivants:             <ol style="list-style-type: none"> <li>a. Conception du code source de l'application</li> <li>b. Gestion des incidents et leur résolution</li> <li>c. Plan de sauvegarde</li> <li>d. Plan de secours</li> </ol> </li> <li>11. Quelle dimension ne fait pas partie de l'architecture de sécurité informatique?             <ol style="list-style-type: none"> <li>a. Dimension technique</li> <li>b. Dimension monétaire</li> <li>c. Dimension organisationnelle</li> <li>d. Dimension juridique</li> </ol> </li> </ol> |
|--|---|

**Exercice 02:**

1. Donner la différence entre l'identification et l'authentification.
2. Quelle est la relation entre : l'authentification, l'intégrité et non-répudiation ?
3. Donner des exemples sur les attaquants dans le monde réel.
4. Pourquoi les pirates s'intéressent-ils aux SI des entreprises?
5. Quelle est la différence entre la sécurité informatique et la cybersécurité ?