

Examen de SSI Ch 1-2

14/10/2025

Test de compréhension de cours de 15 min valant pour 20% de la note d'UE. Répondez aux questions sur la feuille.

NOM et prénom : _____

Formation : _____

/20

1. (3 points) Quel est le rôle de la Sécurité des Systèmes d'Information ?

- ☐ ☒ De réduire l'impact des accidents sur le Système d'Information.
- ☒ ☐ **D'assurer la sécurité des processus métiers du Système d'Information.**
- ☒ ☐ **De répondre aux exigences légales en matière de sécurité des données.**
- ☐ ☒ De supprimer les menaces sur le Système d'Information.
- ☒ ☐ **De réduire l'impact des risques sur le Système d'Information.**
- ☐ ☒ D'assurer la sécurité des utilisateurs du Système d'Information.

Vrai Faux

2. (1 point) Donnez 2 façons pour un attaquant de se faire de l'argent avec un outil de DoS.

Rançon

Sabotage d'un concurrent/Vente de sabotage

3. (2 points) Les lois spécifiques au numérique. . .

- ☒ ☐ **existent.**
- ☐ ☒ sont regroupées dans un code, le Code du Numérique.
- ☒ ☐ **sont (en gros) les mêmes en France et dans l'UE.**
- ☒ ☐ **s'appliquent toujours aux données personnelles des français, même si elles sont stockées en Californie.**

Vrai Faux

4. (1 point) Définissez l'Authentification.

Solution: Vérifier l'identité des acteurs dans un protocole.

5. (1 point) Pour convaincre votre manager, donnez un exemple d'impact d'une attaque sur l'entreprise. Soyez le plus précis possible.

Solution: On peut donner un exemple d'attaque classique, ou des chiffres, ou argumenter que les entreprises victimes de cyberattaques ont généralement du mal à s'en remettre.

On peut aussi discuter de l'impact légal sur l'entreprise.

6. (1 point) Quels sont les critères standards pour mesurer la sécurité ?

Solution: Disponibilité, Intégrité, Confidentialité et Preuve.

7. (1 point) Un audit de sécurité garantit que le Système d'Information est sécurisé.

☐ Oui.

☒ **Non.**

Pourquoi ?

Solution: Il vérifie si le niveau de sécurité est conforme aux réglementations internes et nationales.

8. (1½ points) Associez chaque mécanisme de sécurité et DICP.

Mécanisme	D	I	C	P
Cryptographie		X	X	X
Pare-feu	X		X	
Clauses contractuelles avec les partenaires	X	X	X	X

9. (1 point) Quels sont les risques des entrées-sorties de terminaux personnels dans le réseau interne d'un Système d'Information ?

Solution: Un terminal personnel n'est pas aux normes de sécurité de l'organisme : c'est un maillon faible, plus facile à infecter, qui donne un accès privilégié au réseau interne.

De plus, un utilisateur peut (intentionnellement ou non) faire fuiter des données sensibles à travers son terminal personnel sans être facilement détecté.

10. (1 point) Une attaque est-elle possible sans menace ? Argumentez.

Solution: Non.

Une attaque est une action malveillante portant atteinte à la sécurité d'un Système d'Information. Elle concrétise une menace et utilise une vulnérabilité.

S'il n'y a pas de menace à concrétiser, il n'y a pas d'attaque.

11. (1 point) Pourquoi ne jamais réutiliser son mot de passe de messagerie (mail) ?

Solution: Parce que la boîte mail est très utilisée pour la récupération des accès à d'autres services : l'accès à la boîte mail est un point d'entrée vers beaucoup de vos comptes, il doit être d'autant plus protégé.

12. (2 points) Forcer les utilisateurs de votre application Web à utiliser des caractères spéciaux dans leur mot de passe...

- ☐ ☒ c'est la seule vraie manière d'avoir un mot de passe complexe.
- ☐ ☒ ça pousse les utilisateurs à remplacer les 'a' par des '@', et c'est bien.
- ☐ ☒ c'est plus efficace que d'utiliser des mots de passe longs.
- ☒ ☐ **ça pousse les utilisateurs à ne pas mettre un mot de passe bidon, et c'est bien.**

Vrai Faux

13. (2 points) Une entreprise qui se fait voler des données personnelles de clients doit - légalement - prévenir

- ☒ ☐ **Ses clients.**
- ☐ ☒ Le Fonctionnaire Sécurité Défense.
- ☐ ☒ La gendarmerie.
- ☒ ☐ **Le délégué à la protection des données.**

Vrai Faux

14. (1½ points) Et qu'a le droit de faire le client s'il apprend la nouvelle ?

- ✓ ☐ **Porter plainte auprès de la police.**
- ✓ ☐ **Porter plainte auprès de la CNIL.**
- ☐ ✓ Demander à ce que l'entreprise corrige son erreur en récupérant les données volées.

Vrai Faux