BTS SIO – ÉPREUVE E6 SLAM - SUJET ZÉRO

CAS Lascaux IV

Proposition de corrigé

**Dossier A – Participation à l’atelier d’analyse des risques sur l’application *Web***

***Sous-compétences du bloc 3 mises en œuvre dans ce dossier***

|  |
| --- |
| - Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ;  - Déployer les moyens appropriés de preuve électronique ;  - Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ;  - Identifier les menaces et mettre en œuvre les défenses appropriées ;  - Gérer les accès et les privilèges appropriés ;  - Vérifier l’efficacité de la protection ;  - Caractériser les risques liés à l’utilisation malveillante d’un service informatique ;  - Recenser les conséquences d’une perte de disponibilité, d’intégrité ou de confidentialité ;  - Identifier les obligations légales qui s’imposent en matière d’archivage et de protection des données de l’organisation. |

**Mission A1 – Évaluation des risques à partir des récits utilisateurs**

**Question A1.1**

Indiquer si le tableau contenant les acteurs à l’origine de malveillance est complet. Justifier votre réponse.

Le tableau est incomplet car le guide et le responsable commercial ne sont pas mentionnés. Or, ces partenaires internes à l’entreprise peuvent divulguer des informations confidentielles sur les visiteurs.

**Question A1.2**

Proposer une évaluation des récits utilisateurs 1 et 25 pour chacun des 4 critères (disponibilité, intégrité, confidentialité et preuve).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Intitulé de la *user story* | Disponibilité | Intégrité | Confidentialité | Preuve |
| 1 | En tant qu’acheteur, je veux acheter en ligne les billets pour plusieurs personnes afin de pouvoir participer à une visite. | ***\*\**** | ***\*\**** | ***\*\**** | ***\**** |
| 25 | En tant que responsable commercial, je veux consulter les statistiques de temps passé par zone de visite et les activités réalisées par les visiteurs afin de proposer un meilleur service aux visiteurs. | ***\**** | ***\*\**** | *-* | *-* |

**Question A1.3**

Présenter ces conditions à Christine Berton.

Pour que les traces soient opposables en cas de contentieux, sans ambiguïté possible, leur contenu et leur interprétation doivent être documentés, au sein de la convention de preuve du service d’achat en ligne, dans la politique de traçabilité : pour chaque trace, il convient de décrire dans quel cas elle est produite, les éléments qui y figurent et le sens qu’ils ont**.**

**Mission A2 – Gestion des évènements redoutés**

**Question A.2.1**

Proposer, pour les événements 1 et 3 fournis dans le tableau, les impacts pour l’entreprise et une estimation de leur gravité.

|  |  |  |  |
| --- | --- | --- | --- |
| Numéro de l'événement | Événement | Impact pour l’entreprise | Gravité |
| 1 | Le système ne répond pas. | Perte d’acheteur (de clients)  Mauvaise image de marque | \* |
| 3 | Un attaquant accède à la base de données et modifie l’affectation des guides aux visites. | Désorganisation des visites, perte de réputation | \*\* |

*\* : modérée \*\* : très élevée*

**Question A.2.2**

Proposer des mesures à prévoir lors du développement pour contrer l’évènement redouté numéro 4.

|  |  |  |
| --- | --- | --- |
| Numéro de l'événement | scénario de risque (*abuser story*) | Mesures à prévoir |
| 4 | En tant qu’acheteur, je peux imprimer les billets d’un autre acheteur. | 4.1 Chiffrement du numéro de réservation. |
| 4.2 Vérifier que le numéro de réservation appartient bien à l’acheteur connecté. |

**Question A.2.3**

Proposer un scénario de risque (abuser story) et des mesures à prévoir pour l’événement redouté numéro 3.

|  |  |  |
| --- | --- | --- |
| Numéro de l'événement | scénario de risque (*abuser story*) | Mesures à prévoir |
| 3 | En tant qu’attaquant externe, je peux modifier l’affectation des guides aux visites dans la base de données. | 3.1 Un guide doit être disponible à la date d’une visite. |
| 3.2 Un guide doit parler la langue de la visite à laquelle il est associée. |

**Question A.2.4**

Proposer deux évènements redoutés en lien avec les besoins de sécurité du récit utilisateur (*user story*) 15.

Les événements doivent concerner principalement l’intégrité des données (cf tableau besoins de sécurité)

* Un attaquant accède à la base de données et injecte des commentaires non reliés à un billet ;
* Un attaquant accède à la base de données et ajoute des commentaires diffamatoires.

**Mission A3 – Prise en compte du règlement général sur la protection des données (RGPD) dans les récits utilisateurs**

**Question A3.1**

Lister pour chacun des récits utilisateurs (*user stories*) numérotés 22 et 25, les actions à mettre en œuvre pour respecter le RGPD.

Pour le récit utilisateur numéro 22 :

* Procéder au hachage du mot de passe ;
* Obtenir le consentement préalable du visiteur (*opt-in*) lors de la création de compte ;
* Mettre à disposition les conditions de stockage et d’utilisation des données ;
* Donner la possibilité de supprimer son compte et les données personnelles (photos/vidéos).

Pour le récit utilisateur numéro 25 :

* Gérer les habilitations pour que seul le directeur commercial puisse accéder à la fonctionnalité décrite dans le récit utilisateur.

Dans le cadre du RGPD, la CNIL fait un rappel précis sur le sujet de la « [bonne gestion des habilitations](https://www.cnil.fr/fr/securite-gerer-les-habilitations) » qui s’inscrit dans le RGPD. Une entreprise doit vérifier :

* + que les données qu’elle traite sont nécessaires à ses activités ;
  + qu’aucune donnée dite « sensible » n’est traitée ou, si c’est le cas, qu’elle a bien le droit de les utiliser ;
  + que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
  + qu’elle ne conserve pas des données au-delà de ce qui est nécessaire.
* Établir une fiche de registre relative au traitement des statistiques.

**Question A3.2**

Expliquer quel risque de sécurité vient contrer cet ajout.

Cet ajout permet de contrer le risque d’usurpation d’identité.

**Dossier B – Sécurisation des données**

***Sous-compétences du bloc 3 mises en œuvre dans ce dossier :***

|  |
| --- |
| - Participer à la vérification des éléments contribuant à la qualité d’un développement informatique ;  - Prendre en compte la sécurité dans un projet de développement d’une solution applicative ;  - Gérer les accès et les privilèges appropriés ;  - Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures ;  - Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel. |

**Mission B1 – Vérification de la confidentialité des données**

**Question B.1.1**

a) Identifier les données personnelles présentes sur la représentation conceptuelle de la base de données.

b) Identifier, parmi ces données personnelles, celles qui sont sensibles.

Les données personnelles permettent d'identifier directement ou indirectement une personne.

Les données sensibles forment une catégorie particulière des données personnelles dont le traitement est particulièrement risqué. Il s'agit par exemple des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données concernant la santé ou la vie sexuelle.

1. Identifier les données personnelles présentes sur la représentation conceptuelle de la base de données.

Pour l’entité Acheteur : nom, prenom, mel, telephone, numeroCarteBancaire, motDePasse

Pour l’entité Billet : nom, prenom, dateNaissance, civilite, sexe, mel, estMalentendant, estMalvoyant, qrCode

1. Identifier, parmi ces données personnelles, celles qui sont sensibles

Pour l’entité Billet : estMalentendant, estMalvoyant

**Question B.1.2**

Lister les données devant être chiffrées et celles devant être hachées, pour assurer la confidentialité des données de la table Acheteur.

Données à chiffrer : numeroCarteBancaire, nom, prenom, telephone + mel

Données à hacher : motDePasse

**Question B.1.3**

Réaliser les modifications demandées dans le courriel de Denise Bradord.

1. Select **B.nom, B.prenom, mel**
2. from Acheteur as A
3. join Reservation as R **on R.idAcheteur = A.id**
4. join Billet as B on B.idReservation = R.id
5. join CategorieAge as C on B.idCategorieAge = C.id
6. **join Langue as L on R.idLangue = L.id**
7. where A.id = :par\_idAcheteur
8. and C.libelle = 'senior'
9. and year(dateReservation) = :par\_annee
10. and month(dateReservation) = :par\_mois

**ligne 1 :** remplacer select \* par **select B.nom, B.prenom, mel**

Le select \* fournit toutes les données des tables utilisées par la requête, or seuls le nom, le prénom et l’adresse mail des visiteurs sont nécessaires

**ligne 3** : ajouter **on R.idAcheteur = A.id** pour éviter que toutes les réservations soient prises en compte

**ligne 6** : supprimer la jointure avec Langue, cette table étant inutile car aucune de ses données n’est à prendre en compte pour la requête

Remarque : si la base de données était gérée par un SGBD différent de *MySQL* (SQLServer par exemple), la requête ci-dessus retournerait une erreur de syntaxe mais *MySQL*, plus tolérant à l’égard des comportements non conformes, accepte cette requête au niveau syntaxique.

**Mission B2 – Sécurisation de l’accès à une base de données**

**Question B.2.1**

Justifier la création du compte utilisateur et de ses caractéristiques.

Trois raisons pour justifier ce compte et ses caractéristiques :

* La création d’un compte propre à l’utilisateur, au nom de l’utilisateur, permet d’identifier la personne connectée à la base de données et d’associer une action à un responsable ;
* L’accès à partir d’une machine limite l’accès depuis l’extérieur : l’accès ne pourra se faire qu’à partir d’un poste interne à l’entreprise ;
* La consultation des données des tables autorisées renforce la sécurité car Mme Lesoil dispose uniquement d’un accès en lecture aux tables nécessaires au besoin ;

**Question B.2.2**

Rédiger les requêtes permettant de créer le compte utilisateur et les contraintes de sécurité demandées.

-- création du compte utilisateur qui sera utilisé

CREATE USER 'lesoil'@'172.16.2.1' IDENTIFIED BY 'L#pbGd\M589@';

-- affectation des droits de lecture sur les tables utilisées par la requête :

GRANT SELECT on lascauxprod.CategorieAge to 'lesoil'@'172.15.2.1' ;

GRANT SELECT on lascauxprod.Visite to 'lesoil'@'172.15.2.1' ;

GRANT SELECT on lascauxprod.Billet to 'lesoil'@'172.15.2.1' ;

GRANT SELECT on lascauxprod.Commentaire to 'lesoil'@'172.15.2.1' ;

On évaluera le mot de passe choisi et la connexion de l’utilisateur à partir de la machine autorisée.

**Question B.2.3**

Rédiger une courte note expliquant l’intérêt d’une vue en terme de sécurité.

Seules les données fournies par la vue sont visualisables.

Avec une vue, l’utilisateur Lesoil n’aurait accès qu’aux données fournies par celle-ci. Il lui serait, de ce fait, impossible de faire une autre requête et donc d’accéder à des données sensibles.

**Question B.2.4**

Expliquer en quoi la modération des commentaires est un enjeu important pour Lascaux IV.

La modération des commentaires permet de garantir l’image numérique (e réputation) de Lascaux.

La modération permet de contrôler et superviser les publications des internautes pour préserver l’image de l’entreprise sans empêcher la liberté des échanges.

L'e réputation, présente des enjeux économiques importants tant en terme d'avantages (elle contribue par exemple à la fidélisation de la clientèle) qu'en terme de risques (détérioration de l'image, etc.). La modération des commentaires par le contrôle et la supervision des publications négatives des internautes sur les guides contribue à réduire ces risques et permet de préserver l’image de l’entreprise sans empêcher la liberté des échanges.

**Question B.2.5**

Proposer à Roger Zanches une requête pour répondre à son besoin.

SELECT COUNT(\*)

FROM commentaire

WHERE idBillet IS NULL

Remarque : on exigera la présence du comptage, étant donné que l’on demande uniquement de rechercher l’existence de commentaires non reliés à un billet. Un select ramenant des lignes de la table Commentaire n’est pas approprié ici, au regard du besoin.

**Mission B3 – Adaptation de la représentation conceptuelle de la base de données**

**Question B.3.1**

Identifier et justifier les données devant être supprimées pour une mise en conformité vis à vis de la fiche de registre établie par le DPO.

Suppression de la date de naissance. Cette date est saisie mais elle n’a pas besoin d’être enregistrée : elle permet simplement de déterminer la tranche d’âge du visiteur en vue de définir le tarif du billet (déjà réalisé grâce à l’association entre Billet et CategorieAge).

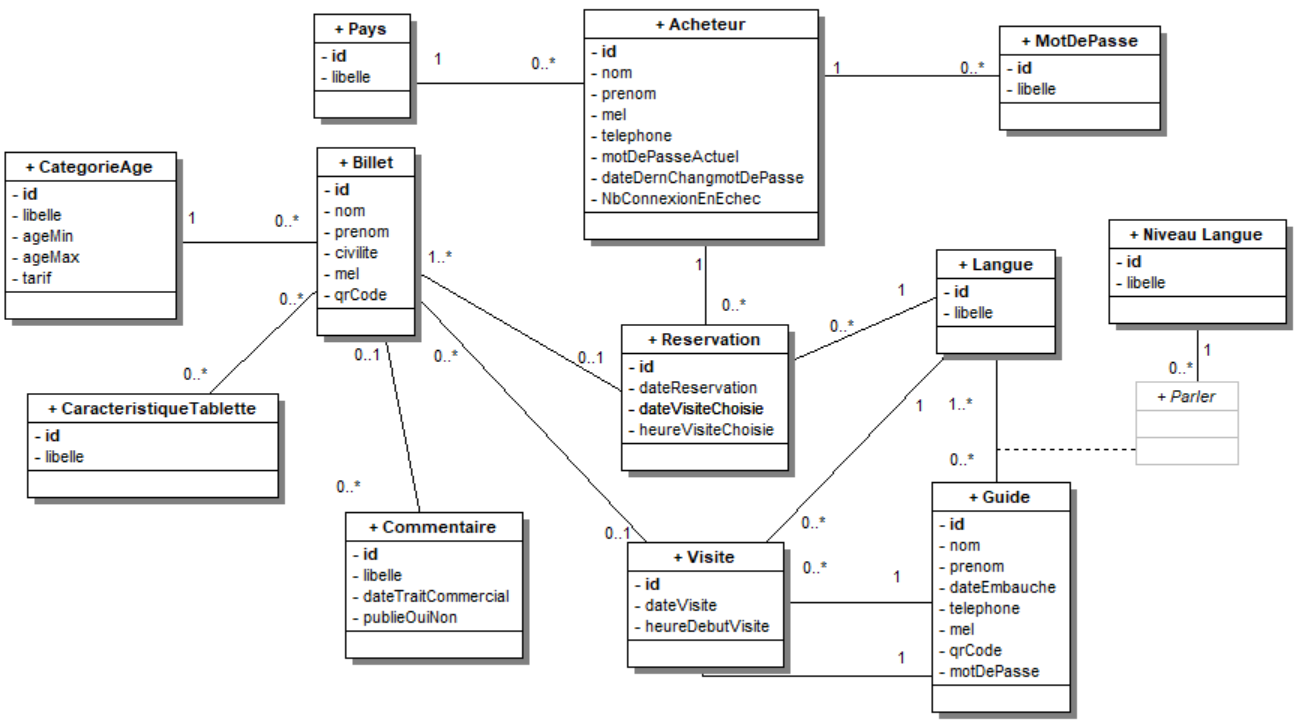
Suppression des coordonnées bancaires car elles ne servent que pour le paiement.

Suppression du sexe car il peut être déduit de la civilité.

**Question B.3.2**

Proposer les modifications à réaliser pour répondre aux nouvelles exigences. Seuls les éléments du schéma existant qui sont concernés par l’évolution seront repris dans le schéma proposé.

Éléments de corrigé du diagramme de classes intégrant le corrigé des questions B3.1 et B3.2 :



Remarque : les attributs nommés ‘id’ sont des identifiants.

**Dossier C – Gestion de la connexion des utilisateurs sur le compagnon de visite (CDV)**

***Sous-compétences du bloc 3 mises en œuvre dans ce dossier***

|  |
| --- |
| - Participer à la vérification des éléments contribuant à la qualité d’un développement informatique  - Prendre en compte la sécurité dans un projet de développement d’une solution applicative  - Prévenir les attaques  - Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel  - Identifier les menaces et mettre en œuvre les défenses appropriées |

**Mission C1 – Identification des visiteurs**

**Question C.1.1**

Identifier les faiblesses du script *getVisiteur.php* du point de vue de la cyber sécurité, en expliquant leurs conséquences possibles sur le système.

Il y a plusieurs faiblesses ici :

1. Le script *getVisiteur.php* ne devrait pas appeler la fonction *getVisiteurByQrCode* sans avoir préalablement filtré l'argument à passer.

Code (non exigé) permettant de corriger ces faiblesses :

header("content-type: application/json; charset=utf-8");

*// vérifie que le champ qrcode est passé en post et renseigné*

if (filter\_has\_var(INPUT\_POST, 'qrcode') == true) {

*// filtre l’argument à passer*

$qrcodeFiltre = filter\_input(INPUT\_POST, 'qrcode', FILTER\_SANITIZE\_STRING) ;

echo getVisiteurByQrCode($qrcodeFiltre);

} else {

$erreur['erreur'] = "absence de code QR";

echo json\_encode($erreur);

}

La technique de filtrage permet de se prémunir contre ces attaques qui pourraient avoir des conséquences graves de corruption et d'effacement de données.

1. La fonction *getVisiteurByQrCode* ne respecte pas bien son contrat :

* Le code de la fonction n'est pas suffisamment sûr et permettrait une attaque de style "injection SQL". La technique de requête préparée permet de se prémunir contre ces attaques qui pourraient avoir des conséquences graves de corruption et d'effacement de données.
* la fonction *getVisiteurByQrCode* ne teste pas le cas où le visiteur n'est pas trouvé dans la base de données

$ligne = $req->fetch(PDO::FETCH\_ASSOC);

if ($ligne == false) {

$erreur['erreur'] = “Pas de visiteur avec ce code QR”;

return json\_encode($erreur);

} else {

return json\_encode($ligne);

}

**Question C.1.2**

Modifier le script *getVisiteur.php* en utilisant une requête préparée.

$qrCode = filter\_input(INPUT\_POST, 'qrcode', FILTER\_SANITIZE\_STRING) ;

$sql = "SELECT billet.id as id, civilite, nom, prenom, mel,

categorieAge.id as idCategorieAge, libelle AS libCategorieA

FROM billet

JOIN CategorieAge ON idCategorieAge = CategorieAge.id

WHERE **qrCode = :qrCode**";

$req = $conn->prepare($sql);

$req->bindValue(':qrCode', $qrCode, PDO::PARAM\_STR);

$req->execute();

La première instruction n’est pas exigée, mais les bonnes pratiques conseillent d’utiliser la fonction filter\_input pour supprimer les balises et les caractères spéciaux des données transmises dans $\_POST.

**Question C.1.3**

Décrire les mesures à mettre en place pour éviter qu'un visiteur peu scrupuleux puisse scanner un billet trouvé par terre ou dans une poubelle et ainsi effectuer une visite avec un billet déjà utilisé.

Plusieurs solutions sont envisageables :

* Vérifier que le billet n’a pas encore été flashé en appelant la méthode isBilletUtilise() de la classe Visiteur. Cet appel se fera dans la méthode *identifierVisiteur* de la classe MainActivity ;
* Contrôler que la date et l’heure de la visite ne sont pas antérieures au moment où le billet est scanné ;
* Modifier la requête SQL située dans la fonction *getVisiteur.php* pour vérifier que le billet n’est pas affecté à une visite

**Mission C2 – Authentification des guides**

**Question C.2.1**

Rédiger la méthode *doitChangerMdP*() de la classe Guide.

public boolean doitChangerMdP(){

*// on récupère la date du jour*

LocalDate dateLimite = LocalDate.now();

*// on calcule la date un trimestre avant*

dateLimite = dateLimite.minusMonths(3);

return this.actuelMotDePasse.getDateCreation().isBefore(dateLimite);

}

**Question C.2.2**

Modifier la méthode *setMotDePasse*() de la classe Guide afin de prendre en compte la nouvelle contrainte de sécurité demandée lors de cette nouvelle itération (*sprint*).

public boolean setMotDePasse(String unMotDePasse){

boolean modifRealisee = true;

**LocalDate aujourdhui = LocalDate.now();**

//1-Vérifier que le mot de passe n'est pas le même que l'actuel

if(unMotDePasse.equals(this.actuelMotDePasse.getMotDePasse()){

modifARealiser = false;

}else{

//2-vérifier que le mot de passe n'a pas été utilisé durant les 12 derniers mois

**LocalDate douzeMoisAvant = aujourdhui.minusMonths(12);**

**for(MotDePasse mdp : this.lesAnciensMotsDePasse){**

**if(mdp.getDateCreation().isAfter(douzeMoisAvant) &&**

**mdp.getMotDePasse().equals(unMotDePasse)){**

**modifARealiser = false;**

**break;**

**}**

}

//3-Si ok on archive le mot de passe actuel et on met à jour le nouveau mot de passe

**if(modifARealiser){**

//On archive le mot de passe actuel

this.lesAnciensMotsDePasse.add(this.actuelMotDePasse);

//Mise à jour du nouveau mot de passe

this.actuelMotDePasse = new MotDePasse(**aujourdhui**, unMotDePasse);

}

return modifARealiser;

}

On peut également utiliser un for pour parcourir l’historique comme ceci :

int tailleHisto = this.lesAnciensMotsDePasse.size() ;

for (int i = 0; i < tailleHisto && modifARealiser) {  
 MotDePasse mdp = this.lesAnciensMotDePasse.get(i);  
 [...]

}

Remarque : La solution présentée ici utilise le parcours de collection proposé dans le sujet, mais d’autres solutions sont possibles comme l’utilisation d’une boucle “tant que non trouvé”, ou de filtrage (stream, filter et lambda expression) par exemple.

**Question C.2.3**

Argumenter en faveur ou non de cette durée.

Si l’on souhaite que le guide ne puisse pas utiliser un de ses anciens mot de passe, il n’y a aucune raison d’exclure les plus anciens, car ces derniers sont tout aussi vulnérables que les plus récents. Donc, la recherche devrait se faire sur tous les anciens mots de passe connus du guide.

**Dossier D – Préparation du développement et pilotage de la sous-traitance**

***Sous-compétences du bloc 3 mises en œuvre dans ce dossier :***

|  |
| --- |
| - Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel  - Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel  - Sensibiliser les utilisateurs à la protection des données à caractère personnel  - Informer les utilisateurs sur les risques associés à l’utilisation d’une ressource numérique et promouvoir les bons usages à adopter  - Identifier les menaces et mettre en œuvre les défenses appropriées  - Gérer les accès et les privilèges appropriés  - Appliquer les procédures garantissant le respect des obligations légales  - Prendre en compte la sécurité dans un projet de développement d’une solution applicative  - Prévenir les attaques |

**Mission D1 – Rejet des mauvaises pratiques de développement**

**Question D.1.1**

Relever les numéros des propositions qu’il faut rejeter à tout prix et justifier votre position pour chacune des propositions rejetées.

**Les propositions 1, 2, 4 et 6 sont à rejeter.**

Proposition 1 : le compte *root* dispose de tous les droits sur toutes les bases de données du serveur. Il est vivement déconseillé dans les scripts d’utiliser le compte *root* pour se connecter à la base de données. Un compte spécifique doit être créé pour l’application ayant uniquement les droits en *select, insert, update, delete* sur les tables de la base de données utilisées par l’application.

Proposition 2 : l’identifiant et le mot de passe de l’administrateur de l’application en production ne doit pas être divulgué aux développeurs.

Proposition 4 : les développeurs ne doivent jamais tester sur des bases de production, ils doivent disposer de bases de test contenant des données différentes des données de production.

Proposition 6 : l’activité des hackers est souvent concentrée les week-ends, il ne faut surtout pas arrêter les éléments de surveillance à ce moment-là.

**Mission D2 – Rédaction d’un contrat de sous-traitance**

**Question D.2.1**

Lister au moins trois préconisations qui devront apparaître dans la partie règle de sécurité du contrat des sous-traitants devant effectuer des interventions sur le site de Lascaux IV.

Générer des comptes avec des restrictions pour chaque intervenant externe.

Mettre en place un cahier de suivi des interventions.

Interdire la mise en place des logiciels de contrôle à distance.

Mettre en place une clause de confidentialité.

Ne fournir au prestataire que les données nécessaires à leur intervention et, pour les données de type client, prévoir un jeu de test ne reprenant pas les vraies identités.

Vérifier que les intervenants sont sensibilisés aux règles de sécurité informatique.

Ne donner accès qu’au lieu, machine et programme concernés par l’intervention.

Désigner un responsable chargé de vérifier le bon déroulement des interventions.

Toute autre proposition judicieuse peut être acceptée.