CCN-CERT

BP/24

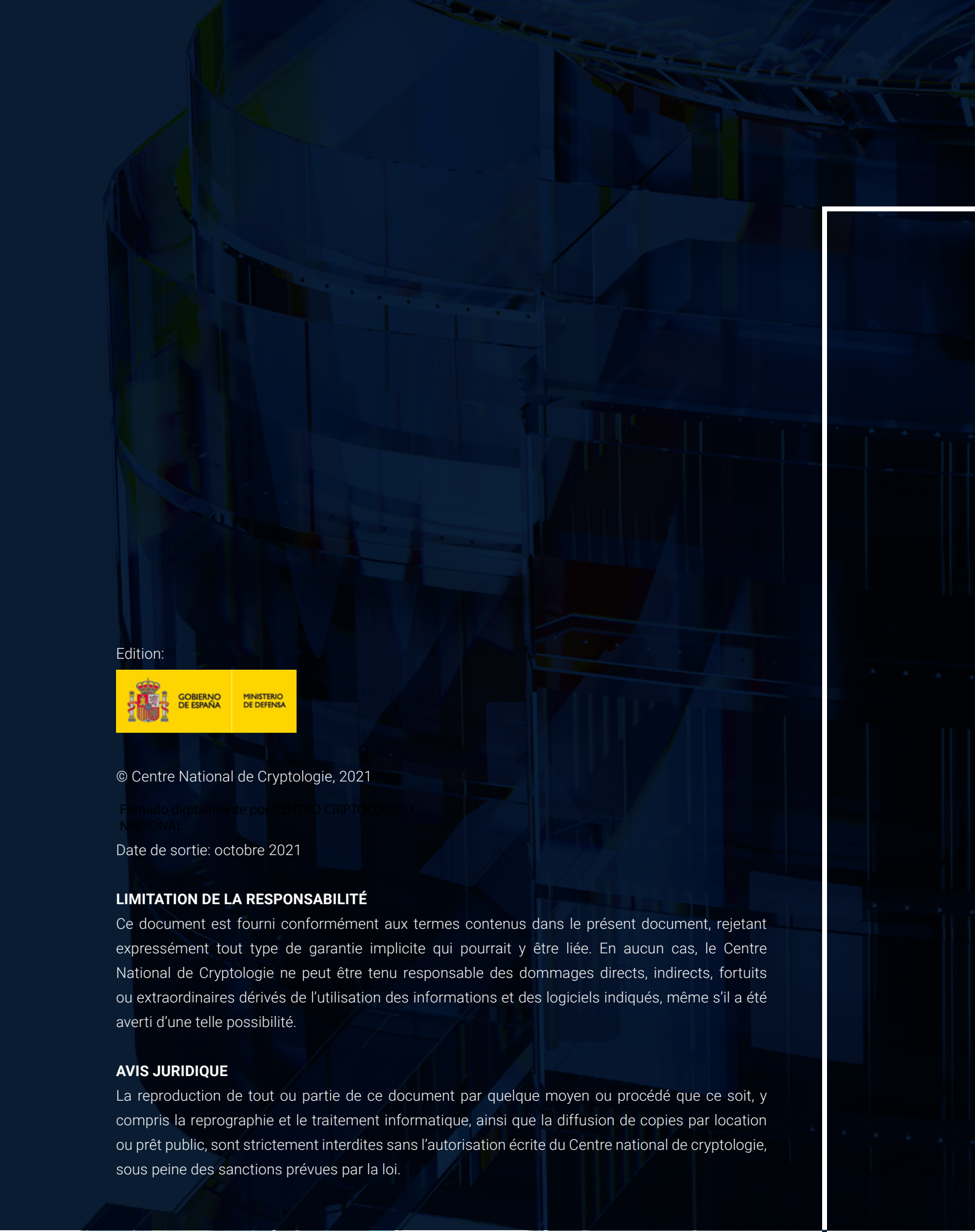
Recommandations pour la sécurité des bases de données

RAPPORT DE BONNES PRATIQUES

DÉCEMBRE 21

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edition:

Date de sortie: octobre 2021

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément tout type de garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et des logiciels indiqués, même s'il a été averti d'une telle possibilité.

AVIS JURIDIQUE

Index

1. À propos du CCN-CERT, Certificat Gouvernemental National **4**
2. Principes fondamentaux de la sécurité des bases de données **5**
3. Mise en œuvre d'une base de données sécurisée **7**
4. Configuration sécurisée de la base de données **8**
4.1. Contrôle d'accès 8
4.1.1 Contrôle des comptes utilisateurs 10
4.1.2 Rôles et groupes 12
4.2. Audit 14
4.3. Les mesures de protection des communications 15
4.4. Mesures de protection des informations 17
4.4.1 Contrôle d'accès basé sur les lignes et les colonnes 17
4.4.2 Contrôle d'accès basé sur des étiquettes 19
4.4.3 Masquage dynamique des données 21
4.4.4 Politiques de sauvegarde 22
4.4.5 Cifred 23
4.5. Revue de logiciel 25
5. Glossaire **26**
6. Tableau récapitulatif des mesures d'amélioration de sécurité **29**

1. À propos du CCN-CERT, Certificat Gouvernemental National

CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN.

Le **CCN-CERT** est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT Gouvernemental National Espagnol** et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de **contribuer à l'amélioration de la cybersécurité espagnole,** en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

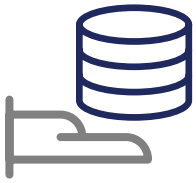
2. Principes fondamentaux de la sécurité des bases de données

Les bases de données constituent généralement l'une des principales cibles des attaques, car elles contiennent des informations sensibles. Il est conseillé de mettre en œuvre une série de directives en matière de sécurité tout en respectant la législation sur la sécurité et la confidentialité.

Les systèmes de gestion de bases de données fonctionnent sur des plates-formes et des systèmes d'exploitation spécifiques qui leur fournissent les éléments fondamentaux de communication et d'accès.

Le modèle de sécurité d'un système de gestion de base de données est divisé en deux domaines d'action:

L'étendue de la plate-forme où le service est exécuté.



L'environnement et les capacités fournis par le gestionnaire de base de données lui-même.

Au niveau de la plate-forme où le service est exécuté, les aspects de sécurité qui sont configurés au niveau du système d'exploitation, tels que les utilisateurs, les services, les communications et les protocoles, peuvent être examinés.

D'autre part, dans l'environnement et les capacités fournis par le gestionnaire de base de données, des aspects tels que les processus d'autorisation et le contrôle d'accès aux données résidant dans les différentes bases de données, le bastionnement des services, les politiques de sauvegarde, le cryptage des données en transit ou au repos, l'audit, etc. peuvent être examinés.

Quelle que soit la technologie du produit de base de données à déployer (Oracle, DB2, SQL, SQL Server, etc.), un certain nombre de recommandations doivent être respectées pour préserver la sécurité des informations et l'intégrité des bases de données en cas d'incident de sécurité hypothétique.

Une fois le processus d'installation effectué, qui diffère selon la technologie déployée, il convient d'appliquer les recommandations de sécurité suivantes, regroupées en différentes catégories, en fonction de l'étendue de la plate-forme où le service est exécuté ou de l'environnement et des capacités fournies par le gestionnaire de la base de données.

Un certain nombre de recommandations doivent être respectées afin de préserver la sécurité des informations et l'intégrité des bases de données en cas d'incident de sécurité hypothétique.

3. Mise en œuvre d'une base de données sécurisée

Au cours du processus d'installation de la base de données, des identifiants d'utilisateur, un groupe et un mot de passe sont créés et leurs valeurs sont généralement implémentées par défaut. Dans le cas où la technologie le permet, il sera nécessaire de les modifier lors de l'installation.

Les gestionnaires de bases de données peuvent utiliser les mécanismes d'authentification propres au système d'exploitation pour identifier et authentifier les utilisateurs. Par conséquent, il est fortement recommandé de spécifier des exigences d'authentification forte au niveau du système d'exploitation.

Il est également recommandé de revoir et de modifier les privilèges par défaut qui ont été accordés aux utilisateurs lors de l'installation. À son tour, il est recommandé de créer des identifiants d'utilisateur propriétaire d'instance spécifiques à chaque instance, en l'ajoutant uniquement en tant que membre du groupe propriétaire d'instance et en ne l'utilisant dans aucun autre groupe. Cela permet de mieux contrôler le nombre d'utilisateurs et de groupes qui peuvent modifier une instance.

Enfin, lors de l'installation des gestionnaires de bases de données, il est recommandé d'utiliser des mots de passe forts, conformes aux politiques de sécurité de l'organisation. Ces caractéristiques sont généralement celles que l'on retrouve lors de la création d'un mot de passe : utiliser des lettres majuscules et minuscules, des chiffres, des caractères spéciaux et une certaine longueur.

4. Configuration sécurisée de la base de données

L'information est un actif qui doit être protégé par **la mise en œuvre de mesures préventives qui protègent l'intégrité et la confidentialité des données.** La conservation et le traitement des informations doivent être considérés comme l'épine dorsale d'une stratégie de sécurité afin de réduire l'exposition aux attaques et d'éviter toute fuite de données indésirable.

4.1 Contrôle d'accès

Les mesures de sécurité axées sur l'accès à une ressource **doivent être précises dans le contrôle d'accès et adaptées aux besoins d'exploitation des données par les utilisateurs.** En conséquence, le risque d'accès non autorisé et de fuite d'informations est considérablement réduit.

Avec des paramètres de contrôle d'accès appropriés, vous pouvez déterminer quels utilisateurs ont accès à quelles données, et même quelles opérations ils peuvent effectuer sur ces données.

Les règles de sécurité et d'autorisation doivent être définies.

Il doit exister un moyen de vérifier **les demandes d'accès** par opérations demandées, données demandées et utilisateurs demandeurs, conformément aux règles de sécurité applicables.

- Le système doit être capable de **reconnaître l'origine d'une demande de l'utilisateur** afin de décider quelles règles de sécurité sont applicables à une certaine demande.
- L'administrateur de la base de données devrait être le personnage qui **ne peut effectuer que les actions suivantes:**
  - **Créer des comptes d'utilisateurs** pour l'accès aux bases de données.
  - **Accorder et annuler des privilèges** aux comptes d'utilisateurs.
  - Attribuer des comptes d'utilisateurs à des **niveaux de sécurité ou d'accréditation.**

L'authentification est le processus par lequel un système vérifie l'identité d'un utilisateur au moyen de protocoles d'authentification tels que LDAP, TNS, SSL, Kerberos, etc.

Il est recommandé de mettre en œuvre les mesures nécessaires pour délimiter la responsabilité dans chaque système lorsqu'il existe des systèmes interconnectés, où l'identification a lieu dans différents domaines de sécurité.

L'authentification est le processus par lequel un système vérifie l'identité d'un utilisateur au moyen de protocoles d'authentification tels que LDAP, TNS, SSL, Kerberos, etc. Les mécanismes d'authentification sont basés sur **"quelque chose que vous savez",** comme les mots de passe ou les clés convenues, **"quelque chose que vous avez"**, comme **les composants logiques** (certificats, systèmes OTP), **les dispositifs** physiques (jetons) et **"quelque chose que vous êtes"**, **comme les éléments biométriques.**

Les facteurs d'authentification utilisés dans le système sont appelés **"justificatifs".** Avant que les utilisateurs ne possèdent des informations d'authentification, ils doivent être identifiés de manière fiable dans le système.

L'accès à une instance ou à une base de données nécessite une authentification de l'utilisateur. Selon le gestionnaire de base de données, l'authentification peut être configurée à l'aide des mécanismes activés par le système d'exploitation, des mécanismes propres au gestionnaire de base de données ou d'une configuration mixte. Dans tous les cas, **il est recommandé d'assurer les contrôles d'accès définis ci-dessus.**

4.1.1 Contrôle des comptes utilisateurs

Les comptes d'utilisateurs par défaut **constituent un vecteur d'attaque évident pour toutes les solutions de bases de données existantes**. Ils doivent donc répondre à certains critères de sécurité afin de minimiser leur exposition et leur exploitation éventuelle.

La **sécurité des comptes utilisateurs** doit répondre aux critères suivants:

- **Séparation des Privilèges et Exposition Minimale.** Les autorisations ne doivent être accordées qu'aux objets auxquels l'accès doit être accordé.
- Une attention particulière doit être portée aux **privilèges accordés**, en veillant à ce que seuls ceux qui sont nécessaires soient attribués.
- Il est recommandé de **créer des identifiants d'utilisateur propriétaire d'instance spécifiques** à chaque instance, en l'ajoutant uniquement en tant que membre du groupe qui possède l'instance et en ne l'utilisant dans aucun autre groupe. Cela permet de mieux contrôler le nombre d'utilisateurs et de groupes qui peuvent modifier l'instance.
- Les directives recommandées **pour la sécurité des mots de passe des comptes utilisateurs** sont les suivantes:
  - **Contenir au moins 12 caractères.**
  - **Incluez des lettres majuscules, au moins deux.**
  - **Contenir au moins deux lettres minuscules.**
  - **Contenir au moins deux chiffres.**
  - **Contenir au moins deux caractères spéciaux.**
  - **Ne contiennent pas le nom de l'utilisateur.**
  - **Durée de vie maximale d'un mot de passe avant d'en forcer le changement: 180 jours.**
- **Blocage du compte.** Les paramètres doivent être configurés pour déterminer:
  - Nombre de tentatives de connexion échouées autorisées avant que le compte de l'utilisateur ne soit verrouillé.
  - Nombre de jours pendant lesquels un compte sera bloqué après une série de tentatives de connexion infructueuses.

Définir une limite de temps de session active pour tous les comptes sur le serveur d'application.

Définissez un nombre limité de sessions par utilisateur pour les comptes de serveurs autres que de base de données.

Définir un temps de déconnexion d'inactivité pour les comptes de serveur non d'application.

Des comptes d'utilisateurs spécifiques doivent être configurés pour les serveurs d'application.

Les comptes utilisateurs doivent être nominatifs afin de garantir la traçabilité des différentes actions exécutées dans le moteur. Il ne faut pas utiliser de comptes génériques associés aux différents rôles, mais plutôt des comptes qui identifient sans équivoque l'auteur de tout changement.

Il est souhaitable de disposer d'un **certificat d'utilisateur pour chaque compte ayant accès au moteur.**

Il est recommandé de mettre en place une authentification à deux facteurs au moteur de la base de données pour les comptes de serveurs d'applications, avec des logins tels que Google Authenticator ou d'autres réseaux sociaux (Social Sign-In Authentication). Ceci est recommandé pour les serveurs d'applications où un nombre indéterminé d'utilisateurs se connecteront.

4.1.2 Rôles et groupes

Lors de la création des objets de la base de données, des autorisations peuvent être accordées sur chaque objet à l'aide d'instructions précises basées sur le principe du moindre privilège.

Les comptes d'utilisateurs doivent être associés à des types ou à des rôles. Les rôles ou types de comptes minimums définis par le fabricant sont les suivants:

Utilisateurs typiques de bases de données: ils sont généralement limités à leur schéma qui contient leurs tables, vues, index et procédures stockées.

Comptes d'application: utilisés pour exécuter vos propres applications et celles de tiers.

Administrateurs des demandes: Ces comptes sont utilisés pour administrer, corriger les vulnérabilités et mettre à jour l'application. Ils doivent donc avoir un accès complet à toutes les données et procédures stockées utilisées pour l'application.

Analystes de données ou utilisateurs de business intelligence: ces utilisateurs ont généralement un accès illimité en lecture au schéma de l'application sans passer par les contrôles d'accès au niveau de l'application.

Administrateurs de bases de données (DBA): ils sont responsables d'une grande variété de tâches liées aux bases de données, notamment la gestion des performances, le diagnostic et le réglage, la mise à jour et la correction des vulnérabilités, le démarrage et l'arrêt de la base de données et la sauvegarde de celle-ci. Votre accès hautement privilégié à la base de données vous donne également accès à toute donnée sensible contenue dans la base de données (dossiers personnels, dossiers médicaux, dossiers financiers de l'entreprise, etc.), bien que cet accès ne soit pas nécessaire pour effectuer des tâches de DBA.

Administrateurs de sécurité: assumez les responsabilités des administrateurs de sécurité, notamment la gestion des comptes d'utilisateurs, la gestion des clés de chiffrement et la gestion des audits.

Il est donc recommandé que:

- Examiner et modifier les privilèges par défaut accordés aux utilisateurs lors de l'installation du gestionnaire de base de données.
- En aucun cas, un compte associé à la fois au rôle de **DBA** et au rôle d'administration de la sécurité ne doit être généré. Deux comptes nominatifs différents doivent être générés si les pouvoirs des deux rôles doivent être donnés à la même personne physique afin d'améliorer la gestion de la séparation des rôles.
- Les comptes d'utilisateurs affectés aux serveurs d'applications ne doivent pas avoir de quotas.
- Il est recommandé de révoquer le privilège de créer des bases de données pour tous les utilisateurs, à l'exception de l'utilisateur **DBA**.
- Il est recommandé d'examiner, et si nécessaire de révoquer, les autorisations des utilisateurs ou des groupes qui n'en ont pas besoin, y compris les privilèges **DBA**.
- Il est recommandé de vérifier qu'aucun accès public n'a été accordé à une base de données.
- Il est recommandé de contrôler l'accès aux données sensibles au niveau des enregistrements, des colonnes, des lignes ou des cellules **(RCAC et RLS).**
- Il est recommandé de configurer le contrôle d'accès par étiquette **(LBAC, RBAC).**

4.2 Audit

L'audit est un élément fondamental pour renforcer la sécurité d'un environnement informatique, en particulier dans les environnements multi-utilisateurs, où il est nécessaire de connaître les actions effectuées par chacun des utilisateurs.

La surveillance de l'accès des utilisateurs individuels et des applications, y compris les actions d'administration du système, peut fournir un enregistrement historique de l'activité du système de base de données.

La fonction d'audit **permet d'auditer au niveau de l'instance** ainsi qu'au **niveau de la base de données individuelle**, toutes les activités étant enregistrées indépendamment dans des journaux séparés pour chacune d'elles.

L'audit est un élément fondamental pour renforcer la sécurité d'un environnement informatique.

- Pour chaque catégorie, **des politiques d'audit peuvent être générées pour enregistrer les échecs, les succès ou les deux.** Il convient de noter que l'activation de toutes les catégories et de tous les événements peut entraîner une surdéclaration et un nombre élevé d'enregistrements.
- Il est recommandé **d'examiner les besoins en matière de journalisation des événements d'audit et de ne retenir que les événements importants** pour l'organisation ou ceux qui sont liés à la sécurité du système.
- Il est recommandé de **créer un rôle AUDITOR et d'accorder les privilèges** nécessaires pour lire et gérer les événements d'audit.
- Il est recommandé de **contrôler l'accès au rôle AUDITOR par le biais de contextes de confiance.** Cela permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
- Il est recommandé que **les fichiers d'audit générés ne soient pas copiés, modifiés ou supprimés** directement par l'administrateur du système d'exploitation ou par tout autre utilisateur non autorisé de la plate-forme.
- Il est recommandé de **crypter les enregistrements de création stockés sur disque (données au repos)**, à la fois sur le serveur de base de données et sur le service de centralisation des journaux, s'il existe.

- Il est recommandé **d'auditer l'accès contrôlé à la clé de cryptage des sauvegardes.**
- Il est recommandé **d'auditer toutes les actions du DBA.**
- Il est recommandé **d'auditer l'accès des utilisateurs,** en particulier ceux qui ont accès à des données sensibles.
- Il est recommandé **d'auditer tous les accès aux tables importantes.**
- Il est recommandé **d'auditer toutes les tentatives de création de base de données.**
- Il est recommandé **d'intégrer les pistes d'audit dans un outil SIEM qui permet de corréler les événements en temps réel,** d'analyser les données et de fournir la capacité technique d'enquêter sur les incidents de sécurité.

4.3 Mesures de protection des communications

Les mesures de sécurité du réseau sont les contrôles de sécurité qui sont ajoutés pour protéger la confidentialité, l'intégrité et la disponibilité des informations. Les recommandations suivantes portent sur les mesures à prendre pour protéger les données en transit avec le plus haut degré de fiabilité.

- Activez l'utilisation de **TLS 1.2** ou supérieur et limitez l'utilisation de **SSL, TLS 1.0** ou **TLS 1.1** sur les réseaux utilisant **TCP/IP**.
- Mise en œuvre et configuration de **pare-feu.**
- Il est recommandé d'utiliser des jeux **d'algorithmes de chiffrement robustes** approuvés par le Centre National de Cryptologie.
- Il est recommandé **d'utiliser des certificats émis par une autorité de certification de confiance.**

- Il est recommandé de modifier les ports par défaut du fabricant.
- Il est recommandé de configurer des listes blanches et noires d'IP ainsi que des plages ayant accès au serveur.

Le service d'écoute surveille le trafic réseau entrant et est l'un des composants les plus susceptibles d'être exposés à des attaques par déni de service distribué (DDoS). Les composantes de ce service doivent être sécurisées et auditées.

Un certain nombre de recommandations sur la sécurité du service sont présentées ci-dessous:

- Des mesures **de sécurité doivent être appliquées à l'accès aux fichiers du service.**
- Les **autorisations d'accès aux services doivent être revues.**
- Il est **recommandé de modifier le nom par défaut des fichiers de service.**
- **L'audit doit être activé.**
- Il est recommandé **d'éditer et de modifier les ports par défaut du fabricant**, en modifiant également les permissions dans le **pare-feu.**
- **Le trafic SQL entre le client et le serveur doit être crypté à l'aide d'algorithmes sécurisés. Les algorithmes obsolètes** tels que DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 et RC4_256 doivent être écartés.

4.4 Mesures de protection des informations

Les mesures de protection de l'information comprennent à la fois celles qui sont configurées ou mises en œuvre dans l'environnement du serveur de base de données et dans l'environnement du système d'exploitation qui fait fonctionner le serveur.

4.4.1 Contrôle d'accès basé sur les lignes et les colonnes

Le contrôle d'accès basé sur **les lignes et les colonnes (RCAC)** est une couche de sécurité supplémentaire permettant de contrôler l'accès aux informations contenues dans un tableau, une colonne, une ligne ou une cellule. Grâce à cette fonction, dont la configuration dépend du fabricant, vous pouvez vous assurer que les informations sont protégées de manière adéquate, en veillant à ce que les utilisateurs n'aient accès qu'au sous-ensemble de données dont ils ont besoin pour accomplir leurs tâches.

Avantages du contrôle d'accès basé sur les lignes et les colonnes:

- Le contrôle d'accès basé sur les lignes et les colonnes est conforme au principe du **"besoin de savoir".**
- **Aucun utilisateur de la base de données n'est intrinsèquement exempté des règles de contrôle d'accès aux lignes et aux colonnes.**
- Les **données de la table sont protégées** quelle que soit la manière dont on accède à la **table via SQL.**
- **Les applications,** les outils d'interrogation de fortune et les outils d'établissement de rapports **sont tous soumis à des règles d'accès par ligne et par colonne.** L'application est centrée sur les données.

Le modèle de sécurité basé sur les lignes et les colonnes **se concentre sur qui accède** à quelles **informations**, et non sur un ensemble statique de permissions. Les ensembles de résultats pour une même requête changent en fonction du contexte dans lequel la requête a été demandée et **aucun avertissement ou erreur n'est renvoyé.**

Il est recommandé de concevoir et d'utiliser des politiques d'accès basées sur les lignes et les colonnes dans les environnements où il existe des réglementations ou des normes à respecter et où l'accès aux données doit se faire en fonction du contexte du demandeur.

4.4.2 Contrôle d'accès basé sur des étiquettes

Le contrôle d'accès basé sur les étiquettes **(LBAC)** est un modèle de sécurité qui est principalement destiné aux applications gouvernementales ou aux applications dont les niveaux de classification sont connus, car il exige que les données et les utilisateurs soient classés à l'aide d'un ensemble fixe de règles qui sont mises en œuvre.

Le contrôle d'accès basé sur les balises permet de contrôler qui peut accéder aux données, en augmentant le contrôle sur qui peut lire ou interroger et qui peut modifier les informations des lignes et des colonnes.

Une politique de sécurité basée sur les balises comprend les informations suivantes:

- Quels **composants d'étiquettes de sécurité sont utilisés** dans les étiquettes de sécurité qui font partie de la politique.
- Quelles **sont les règles utilisées pour comparer les composants de l'étiquette** de sécurité.
- Lesquels de certains **comportements facultatifs sont utilisés lors de l'accès** aux données protégées par la politique.
- Quels **sont les labels de sécurité et les exceptions supplémentaires à prendre en compte lors de l'application de l'accès aux données protégées par la politique de sécurité.**

Chaque table protégée doit être associée à une et une seule politique de sécurité. Les lignes et les colonnes de cette table ne peuvent être protégées que par des étiquettes de sécurité qui font partie de cette politique de sécurité et tout accès aux données protégées suit les règles de cette politique.

Vous pouvez avoir plusieurs politiques de sécurité sur une seule base de données, mais vous ne pouvez pas avoir plus d'une politique de sécurité protégeant une table donnée.

Il est recommandé d'utiliser le contrôle d'accès par étiquette au niveau de l'enregistrement lors du **traitement d'informations sensibles** ou **classifiées liées à des entités gouvernementales.**

Le contrôle d'accès par étiquette au niveau des enregistrements est recommandé lorsque les affirmations suivantes sont vraies:

- **Le degré de classification des données est connu.**
- **La classification des données peut être représentée par une ou plusieurs étiquettes de sécurité.**
- **Les règles d'autorisation peuvent être liées aux composants de l'étiquette de sécurité.**

Le contrôle d'accès basé sur les étiquettes de niveau colonne est recommandé lorsque:

- **Les colonnes sensibles doivent être protégées contre tout accès non autorisé** par les propriétaires des tables ou **même par le DBA.**

Il est nécessaire de protéger des tables entières contre tout accès non autorisé aux propriétaires de la table ou même au DBA. Dans ce cas, vous attribuerez une étiquette de sécurité à toutes les colonnes de la table, puis vous attribuerez l'étiquette de sécurité à un rôle et vous assignerez ce rôle uniquement aux utilisateurs qui doivent accéder aux informations de la table.

Indépendamment des contrôles d'accès mis en place, il est recommandé d'utiliser des mécanismes de cryptage au repos pour les données, les tableaux, les fichiers d'audit et les fichiers de sauvegarde au niveau du système d'exploitation.

4.4.3 Masquage dynamique des données

Le masquage des informations est une **fonction qui permet d'anonymiser et de cacher les données,** limitant ainsi l'accès des utilisateurs non privilégiés aux informations les plus sensibles.

Le masquage des données permet de **dissimuler des informations sensibles dans l'ensemble des résultats obtenus** à partir d'une interrogation de champs désignés dans une base de données.

Il est possible de définir des règles de masquage sur une colonne d'une table afin d'obscurcir les données de cette colonne. Cependant, la création d'un masque sur une colonne n'empêche pas les mises à jour de cette colonne. **Il est donc nécessaire de disposer d'une politique de contrôle d'accès appropriée ou d'une politique visant à limiter les autorisations de mise à jour.**

4.4.4 Politiques de sauvegarde

Une sauvegarde est un **processus par lequel des informations existantes sont dupliquées d'un support à un autre, afin de pouvoir les récupérer en cas de défaillance du premier hôte de données.**

Parfois, une mauvaise politique de protection de la sauvegarde permet un accès non autorisé aux informations. Par conséquent, si les données sont protégées par des sauvegardes, il est possible d'y accéder directement à partir du service de sauvegarde de tout gestionnaire de base de données.

Les bonnes pratiques générales suivantes sont exposées ci-dessous, quelle que soit la version du produit.

Il est recommandé de **crypter tous les fichiers de sauvegarde et les images d'archive,** quel que soit le support sur lequel ils sont stockés.

Il est recommandé de veiller à ce que **la restauration de toute sauvegarde nécessite un accès contrôlé à la clé de chiffrement et fasse l'objet d'un audit,** tant pour l'accès que pour la restauration elle-même.

Les pratiques de sauvegarde recommandées par **le fabricant doivent être maintenues.**

Des sauvegardes régulières sont recommandées. Au moins une sauvegarde incrémentielle doit être générée quotidiennement et conservée pendant **sept jours.** Une sauvegarde incrémentielle hebdomadaire doit également être générée le dimanche et conservée pendant quatre semaines. En outre, une copie incrémentielle doit être générée chaque premier jour du mois, les douze derniers mois étant conservés. Enfin, une sauvegarde annuelle doit être **générée et conservée pendant cinq ans.**

Stockez les **sauvegardes dans des endroits autres que l'emplacement physique du serveur de production.**

Il est recommandé **de stocker les sauvegardes sur des systèmes de disques redondants.**

Effectuez régulièrement des tests de **récupération sous la forme d'une marche à vide.**

4.4.5 Cifred

Le cryptage est la conversion de données disponibles dans un format lisible en un autre format codé créant la nécessité de les décrypter pour les traiter. Le cryptage consiste à utiliser une clé cryptographique générée par des valeurs mathématiques acceptées par l'expéditeur et le destinataire pour convertir le contenu d'un message en un format illisible, ce qui permet de protéger l'information contre des agents externes et non autorisés.

Il est de la responsabilité de l'organisation de connaître et de sécuriser les données les plus sensibles en sa possession. Cela dépend du contenu de l'information dans les différentes bases de données. Toutes les données n'ont pas la même criticité et il appartient à l'organisation de catégoriser d'abord les informations, puis d'en sécuriser l'accès en fonction de la sensibilité des données.

Différents protocoles de cryptage sont disponibles en fonction de l'état des informations. Ainsi, le cryptage peut être classé dans les catégories suivantes:

Cryptage en transit: les données sont considérées comme étant en transit lorsqu'elles sont déplacées entre des dispositifs. Lors du transfert d'informations, les données sont exposées à un risque accru en raison de la nécessité de les décrypter avant de les transférer.

Le chiffrement des données pendant le transfert est appelé chiffrement de bout en bout. Le cryptage de bout en bout garantit la protection de la confidentialité des données, même si celles-ci sont interceptées. Il est recommandé d'utiliser des protocoles de cryptage pour le trafic SQL entre clients et serveurs, tels que AES, FIPS, Triple DES, TLS, etc.

Cryptage au repos: les données au repos sont considérées comme telles lorsqu'elles sont collectées et stockées sur des disques durs, des bandes de sauvegarde ou dans le nuage, elles sont considérées comme inactives et stables. Les données au repos doivent toujours être cryptées et peuvent l'être à l'aide de protocoles tels que AES, Triple DES, SHA, etc.

En outre, il est recommandé de crypter l'ensemble de la base de données, les objets de la base de données, les tables, les colonnes, les cellules, les pistes d'audit et toutes les sauvegardes, quel que soit le support sur lequel elles sont stockées.

Le National Cryptologic Centre dispose de guides de configuration spécifiques qui contiennent les détails du cryptage des bases de données parmi d'autres informations pertinentes pour les bases de données Oracle et DB2.

- Recommandations de sécurité pour la base de données oracle 19c.
- Recommandations de sécurité pour les bases de données db2.

4.5 Revue de logiciel

Après l'installation du produit et de ses mises à jour, il faut vérifier l'état de la solution. Les autorisations des objets déjà sécurisés peuvent avoir changé et doivent être vérifiées à nouveau.

Il est important d'examiner la documentation des objets concernés et de les revoir par la suite. Au niveau du logiciel, les tâches de maintenance suivantes doivent être effectuées régulièrement:

- **Maintenez la version du moteur à jour.**
- Maintenez à jour les versions de tout logiciel dépendant du moteur.
- Il est recommandé de configurer des **alarmes pour la consommation et l'utilisation du moteur de BD.**
- Il est recommandé de **documenter toutes les modifications apportées au moteur de BD et les tâches d'administration.**
- Vérifiez que **les comptes utilisateurs ne sont pas root** dans le système d'exploitation.
- **Passez en revue les vulnérabilités de chaque composant de l'installation.** Les vulnérabilités connues **(CVE)** par composant **(CPE)** peuvent être consultées sur des portails tels que le **NIST**.
- Si des vulnérabilités sont publiées et n'ont pas été corrigées par le fabricant, **elles doivent être signalées aux responsables de la sécurité.**
- **Nettoyez les fichiers temporaires** après l'installation d'un produit, une mise à niveau ou la correction d'une vulnérabilité.

5. Glossaire

TLS: Transport Layer Security est un protocole de communication dont l'objectif principal est d'assurer la confidentialité et l'intégrité des données entre deux applications en communication. Le protocole est composé de deux couches : le protocole d'enregistrement TLS et le protocole de poignée de main TLS. Pendant la négociation TLS, un algorithme de clé publique est utilisé pour échanger de manière sécurisée des signatures numériques et des clés de chiffrement entre un client et un serveur. Les informations d'identité et la clé sont utilisées pour établir une connexion sécurisée pour la session entre le client et le serveur. Une fois la session sécurisée établie, la transmission des données entre le client et le serveur est chiffrée à l'aide d'un algorithme symétrique, tel que l'AES.

RCAC: Row and Column Access Control (contrôle d'accès aux lignes et aux colonnes). Il permet de contrôler l'accès à une table au niveau des lignes, des colonnes ou des deux. Il peut être utilisé pour compléter le modèle de privilège de table, en garantissant que les informations sont protégées de manière adéquate et que les utilisateurs n'ont accès qu'au sous-ensemble de données nécessaire à l'exécution de leurs tâches professionnelles et au respect de règles et réglementations spécifiques.

LBAC: Label Based Access Control. Il s'agit d'un modèle de sécurité principalement destiné aux applications gouvernementales ou aux applications dont le degré de classification est connu, car il exige que les données et les utilisateurs soient classifiés à l'aide d'un ensemble fixe de règles qui sont mises en œuvre.

DBA: Administrateur de base de données.

FIPS: Federal Information Processing Standards. La publication 140-2 des Federal Information Processing Standards (FIPS) est une norme du gouvernement américain qui définit les exigences de sécurité minimales pour les modules cryptographiques dans les produits de technologie de l'information, comme défini dans la section 5131 de l'Information Technology Management Reform Act de 1996.

LDAP: Lightweight Directory Access Protocol (protocole d'accès à un répertoire léger) est un protocole de niveau applicatif qui permet d'accéder à un service de répertoire ordonné et distribué pour rechercher des informations dans un environnement de réseau.

5. Glossaire

SSL: Secure Sockets Layer, la technologie standard pour sécuriser une connexion Internet, ainsi que pour protéger toute information sensible envoyée entre deux systèmes et empêcher les criminels de lire et de modifier les données transférées, y compris les informations qui pourraient être considérées comme personnelles.

Kerberos: protocole d'authentification sur réseau informatique créé par le MIT, qui permet à deux ordinateurs sur un réseau non sécurisé de prouver leur identité l'un à l'autre de manière sûre.

OTP: Mot de passe à usage unique utilisé pour l'authentification.

Authentification par signature sociale: Social Sign-In est une authentification unique pour les utilisateurs finaux. Avec les informations de connexion existantes d'un fournisseur de médias sociaux tel que Facebook, Twitter ou Google, l'utilisateur peut se connecter à un site web tiers au lieu de créer un nouveau compte spécifiquement pour ce site.

AES: Advanced Encryption Standard (AES), est un schéma de chiffrement par blocs adopté comme norme de chiffrement par le gouvernement des États-Unis, créé en Belgique. AES a été annoncé par le National Institute of Standards and Technology (NIST) comme US FIPS PUB 197 (FIPS 197) le 26 novembre 2001 après un processus de normalisation de 5 ans. Elle est devenue une norme effective le 26 mai 2002. Depuis 2006, AES est l'un des algorithmes les plus populaires utilisés en cryptographie symétrique.

DES: Data Encryption Standard (DES) est un algorithme de cryptage, c'est-à-dire une méthode pour crypter des informations, choisi comme norme FIPS aux États-Unis en 1976, et dont l'utilisation s'est largement répandue dans le monde.

Triple DES : En cryptographie, Triple DES est le nom donné à l'algorithme qui effectue le cryptage triple DES.

SHA: Les algorithmes de hachage sécurisés1 sont une famille de fonctions de hachage cryptographiques publiées par le National Institute of Standards and Technology (NIST) en tant que norme fédérale américaine de traitement de l'information (FIPS).

5. Glossaire

SIEM: La gestion des informations et des événements de sécurité (SIEM) est un terme de cybersécurité dans lequel les services et les produits logiciels combinent deux systèmes : la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM).

DDoS: En sécurité informatique, une attaque par déni de service, également appelée attaque DoS (Denial of Service), est une attaque sur un système ou un réseau informatique qui rend un service ou une ressource inaccessible aux utilisateurs légitimes.

CVE: Common Vulnerabilities and Exposures (CVE) est une liste d'informations enregistrées sur les vulnérabilités de sécurité connues, dans laquelle chaque référence comporte un numéro CVE-ID, une description de la vulnérabilité, les versions du logiciel qui sont affectées, une solution de contournement possible (le cas échéant) ou la façon de configurer pour atténuer la vulnérabilité et des références à des publications ou à des articles de forum ou de blog où la vulnérabilité a été rendue publique ou son exploitation est démontrée. En outre, un lien direct vers les informations de la base de données sur les vulnérabilités du NIST (NVD), où l'on peut obtenir plus de détails sur la vulnérabilité et son évaluation, est généralement aussi affiché.

NIST: Le National Institute of Standards and Technology (NIST), appelé National Bureau of Standards (NBS) entre 1901 et 1988, est une agence de l'Administration de la technologie du Département du commerce des États-Unis. La mission de cet institut est de promouvoir l'innovation et la concurrence industrielle aux États-Unis grâce aux progrès de la métrologie, des normes et de la technologie, de manière à renforcer la stabilité économique.

RLS: Row-Level Security. La sécurité au niveau des lignes vous permet d'utiliser l'appartenance à un groupe ou le contexte d'exécution pour contrôler l'accès aux lignes d'une table de base de données.

6.Tableau récapitulatif des mesures d'amélioration de sécurité 17

CHAMP	NÚM	MESURE	MOTIF
MISE EN ŒUVRE SÉCURISÉE	1	Sur les systèmes Unix ou Linux, il est recommandé de spécifier des noms d'utilisateur différents de ceux créés par défaut, quel que soit le gestionnaire de base de données à mettre en œuvre.	Évitez d'utiliser les noms par défaut pour planifier des attaques sur la base de données.
	2	Sur les systèmes Windows, il est recommandé de modifier ce paramètre par défaut et de spécifier des noms d'utilisateur différents pour chaque rôle.	Évitez d'utiliser les noms par défaut pour planifier des attaques sur la base de données.
	3	Il est recommandé de créer des identifiants de propriétaire d'instance spécifiques à chaque instance, en l'ajoutant uniquement en tant que membre du groupe de propriétaires d'instance et en ne l'utilisant dans aucun autre groupe.	Avoir plus de contrôle sur le nombre d'utilisateurs et de groupes qui peuvent modifier l'instance.
	4	Pendant l'installation, il est recommandé d'utiliser des mots de passe forts, conformes aux politiques de sécurité de l'organisation.	Réduire au minimum les possibilités d'attaques par force brute.
CONTRÔLE D'ACCÈS	5	Nous recommandons l'utilisation de mots de passe forts et solides contenant au moins 12 caractères, y compris des majuscules, des minuscules, des chiffres et des caractères spéciaux.	Réduire au minimum les possibilités d'attaques par force brute.
	6	Il est recommandé de fixer la durée de vie maximale d'un mot de passe à 180 jours au maximum.	Le temps limite l'attaquant pour compromettre le mot de passe d'un utilisateur.
	7	Il est recommandé de mettre en place des politiques de blocage des comptes.	Limiter les tentatives d'un attaquant d'accéder aux ressources du système.

6. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NÚM	MESURE	MOTIF
CONTRÔLE D'ACCÈS	8	Il est recommandé de configurer des comptes d'utilisateurs spécifiques pour les serveurs d'applications.	Limiter la surface d'attaque.
	9	Il est conseillé d'établir une authentification à deux facteurs.	Renforcer la sécurité de l'identité numérique des utilisateurs.
	10	Il est recommandé d'utiliser des mécanismes d'authentification et de communication forts tels que SERVER, LDAP TLS ou Kerberos.	Améliorer la sécurité et la fiabilité des mécanismes d'authentification.
	11	Il est recommandé de suivre le principe du moindre privilège, selon lequel seuls les utilisateurs sont autorisés à accéder aux informations et à effectuer les actions dont ils ont réellement besoin.	Réduire au minimum la surface d'exposition.
	12	Il est recommandé d'examiner et, si nécessaire, de révoquer les autorisations des utilisateurs ou des groupes qui n'en ont pas besoin.	Réduire au minimum la surface d'exposition.
	13	Dans les scénarios où des données sensibles sont stockées, il est recommandé, en plus de l'examen des privilèges, d'établir des contrôles d'accès granulaires.	Empêcher l'accès aux rôles sensibles depuis des environnements non fiables.
	14	Il est recommandé de révoquer les privilèges d'accès aux données du DBA s'il n'a pas réellement besoin d'accéder aux données.	Par défaut, un DBA a accès à toutes les tables de son instance de base de données. Cela présente un risque, surtout si le compte a été violé ou si ces privilèges sont utilisés de manière abusive.
	15	Il est recommandé de vérifier qu'aucun accès public n'a été accordé à une base de données.	Réduire au minimum la surface d'exposition.
	16	Il est recommandé d'attribuer des privilèges par le biais d'un modèle de rôle, en évitant l'attribution directe aux utilisateurs.	Améliorer le contrôle et la maintenance des privilèges d'accès.
	17	Il est recommandé d'utiliser les contrôles d'accès du système d'exploitation.	Empêcher les administrateurs du système d'exploitation d'obtenir un accès trop important.
	18	Il est recommandé d'attribuer les autorisations DBA uniquement par le biais d'un rôle, et de contrôler l'accès à ce rôle par le biais de contextes de confiance.	Permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
	19	Il est recommandé de révoquer le privilège de créer des bases de données pour tous les utilisateurs sauf le DBA.	Réduire au minimum la surface d'exposition.

6. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NÚM	MESURE	MOTIF
AUDIT	20	Il est recommandé d'examiner les besoins en matière de journalisation des événements d'audit et de ne retenir que les événements importants pour l'organisation ou ceux qui sont liés à la sécurité du système.	Contrôler les informations d'audit générées, en évitant les données non pertinentes et les problèmes de stockage qui peuvent entraîner la perte d'éléments probants pertinents.
	21	Il est recommandé de créer un rôle AUDITOR et d'accorder les privilèges nécessaires pour lire et gérer les événements d'audit.	Contrôlez qui peut accéder aux informations d'audit et comment.
	22	Il est recommandé de contrôler l'accès au rôle AUDITOR par le biais de contextes de confiance.	Permet de limiter l'accès aux seules connexions provenant d'ordinateurs de confiance.
	23	Il est recommandé que les fichiers d'audit générés ne soient pas copiés, modifiés ou supprimés directement par l'administrateur du système d'exploitation ou par tout autre utilisateur non autorisé de la plate-forme.	Empêchez l'exfiltration de données ou l'accès à des informations d'audit sensibles en contournant les mécanismes de sécurité des bases de données.
	24	Il est recommandé d'utiliser un service centralisateur (SIEM) pour les pistes d'audit.	Unification des différentes sources d'audit, facilitant la corrélation des journaux et évitant la perte ou la manipulation des preuves.
	25	Il est recommandé de crypter les enregistrements de création stockés sur disque (données au repos), à la fois sur le serveur de base de données et sur le service de centralisation des journaux, s'il existe.	Empêchez l'exfiltration de données ou l'accès à des informations d'audit sensibles en contournant les mécanismes de sécurité des bases de données.
	26	Il est recommandé d'auditer toutes les actions du DBA.	Conservez une piste d'audit des actions administratives susceptibles de compromettre le système.
	27	Il est recommandé d'auditer l'accès des utilisateurs, en particulier ceux qui ont accès à des données sensibles.	Conserver une piste d'audit des actions des utilisateurs.
	28	Il est recommandé d'auditer tous les accès aux tables importantes.	Conservez une piste d'audit des actions susceptibles de compromettre le système.
	29	Il est recommandé d'auditer toutes les tentatives de création de bases de données.	Conservez une piste d'audit des actions administratives susceptibles de compromettre le système.
	30	Il est recommandé d'auditer l'accès contrôlé à la clé de cryptage des sauvegardes.	Conservez une piste d'audit des actions susceptibles de compromettre les informations.

6. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NÚM	MESURE	MOTIF
PROTECTION DES COMMUNICATIONS	31	Il est recommandé d'utiliser un cryptage avec des algorithmes sécurisés exposés au niveau de la couche de communication, comme TLS 1.2 ou plus.	Empêcher la capture de données en transit sur le réseau.
	32	Il est recommandé de ne pas chiffrer les données en utilisant des algorithmes obsolètes.	Les algorithmes suivants sont dépréciés: DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 et RC4_256 et ne doivent pas être utilisés.
	33	Il est recommandé d'utiliser des jeux d'algorithmes de chiffrement robustes approuvés par le Centre National de Cryptologie.	Empêcher l'exploitation des vulnérabilités des algorithmes faibles ou obsolètes.
	34	Mise en œuvre et configuration de pare-feu.	Renforcer le contrôle du trafic à l'entrée et à la sortie des ports.
	35	Il est recommandé de modifier les ports par défaut du fabricant.	Renforcer la sécurité d'accès.
	36	Il est recommandé d'examiner et de configurer les ports utilisés par toutes les instances du serveur.	Réduisez la surface d'exposition en n'autorisant que les ports de communication nécessaires.
PROTECTION DES INFORMATIONS	37	Il est recommandé de concevoir et d'utiliser des politiques d'accès granulaires aux enregistrements, colonnes ou lignes dans les environnements où il y a des réglementations ou des normes à respecter et où l'accès aux données doit se faire en fonction du contexte du demandeur.	Respecter le principe du "besoin de savoir".
	38	Il est recommandé d'utiliser le contrôle d'accès par étiquette au niveau des enregistrements lors du traitement d'informations sensibles ou classifiées liées à des entités gouvernementales.	Respecter le principe du "besoin de savoir".
	39	Il est recommandé d'utiliser le contrôle d'accès basé sur les balises au niveau des enregistrements lorsque les affirmations suivantes sont vraies: – Le degré de classification des données est connu. – La classification des données peut être représentée par une ou plusieurs étiquettes de sécurité. – Les règles d'autorisation peuvent être liées aux composants de l'étiquette de sécurité.	Respecter le principe du "besoin de savoir".

6. Tableau récapitulatif des mesures d'amélioration de sécurité

CHAMP	NÚM	MESURE	MOTIF
PROTECTION DES INFORMATIONS	40	Le contrôle d'accès basé sur les étiquettes de niveau colonne est recommandé lorsque: – Il est nécessaire de protéger les colonnes sensibles contre les accès non autorisés des propriétaires de la table ou même du DBA. – Il est nécessaire de protéger des tables entières contre tout accès non autorisé aux propriétaires de la table ou même au DBA.	Respecter le principe du "besoin de savoir".
	41	Il est recommandé de limiter l'exposition des informations sensibles en les cachant aux utilisateurs non privilégiés grâce au masquage dynamique des données. La disponibilité de cette fonction dépend du fabricant.	Respecter le principe du "besoin de savoir".
BACKUP	42	Il est recommandé de crypter tous les fichiers de sauvegarde et les images d'archive, quel que soit le support sur lequel ils sont stockés.	Empêcher tout accès non autorisé aux sauvegardes.
	43	Il est recommandé de veiller à ce que la restauration de toute sauvegarde nécessite un accès contrôlé à la clé de chiffrement et fasse l'objet d'un audit, tant pour l'accès que pour la restauration elle-même.	Empêchez tout accès non autorisé aux sauvegardes et enregistrez tout accès par le biais de l'audit.
	44	Stockez les sauvegardes à des endroits autres que l'emplacement physique du serveur de production.	Éviter l'indisponibilité des informations en cas d'attaque ou de défaillance du système.
CIFRED	45	Le chiffrement de l'ensemble de la base de données, des objets de la base de données, des tables, des colonnes, des cellules, des pistes d'audit et de toutes les sauvegardes est recommandé, quel que soit le support sur lequel ils sont stockés.	Protéger la vie privée.
REVUE DE LOGICIEL	46	Il est recommandé de maintenir la version du moteur à jour et le logiciel dépendant.	Corriger les vulnérabilités qui peuvent affecter la base de données.
	47	La configuration des alarmes de consommation et l'utilisation du moteur de base de données sont recommandées.	La surveillance des ressources du système permet d'éviter les erreurs qui peuvent affecter l'accès aux données.

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es