CCN-CERT

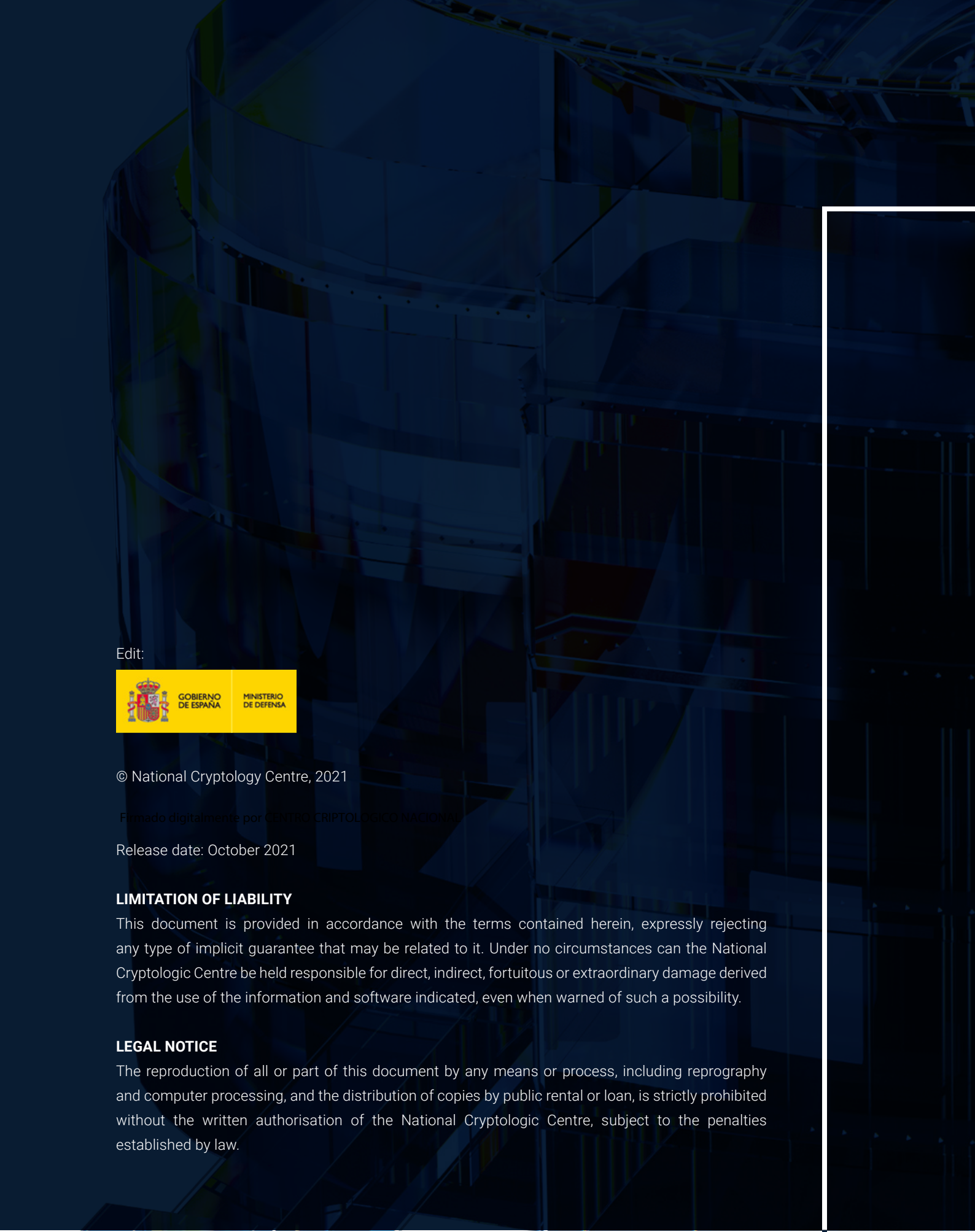
BP/24

Database security recommendations

GOOD PRACTICE REPORT

DECEMBER 2021

ccn-cert centro criptológico nacional
CCN centro criptológico nacional



Edit:

Release date: October 2021

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained herein, expressly rejecting any type of implicit guarantee that may be related to it. Under no circumstances can the National Cryptologic Centre be held responsible for direct, indirect, fortuitous or extraordinary damage derived from the use of the information and software indicated, even when warned of such a possibility.

LEGAL NOTICE

Index

1. About CCN-CERT, National Governmental CERT

CCN-CERT is the Information Security Incident Response Capability of the National Cryptologic Centre, CCN.

The **CCN-CERT** is the Information Security Incident Response Capacity of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Scheme (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity,** being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively face cyber-threats, including the coordination at state public level of the different existing Incident Response Capabilities or Cybersecurity Operations Centres.

All of this, with the ultimate **aim of achieving a more secure and reliable cyberspace**, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Legal Regime of the Public Sector, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incident management will be carried out by the CCN-CERT in coordination with the CNPIC.

2. Fundamentals of database security

One of the main targets of attack is usually databases because they contain sensitive information. It is advisable to implement a series of security guidelines while maintaining compliance with security and privacy legislation.

Database management systems run on specific platforms and operating systems that provide them with the fundamental elements of communication and access.

The security model of a database management system shall be divided into two policy areas:

The scope of the platform where the service runs.

The environment and capabilities provided by the database manager itself.

2. Fundamentals of database security

At the level of the platform where the service is running, security aspects that are configured at the level of the operating system, such as users, services, communications and protocols, can be reviewed.

On the other hand, in the environment and capabilities provided by the database manager, aspects such as authorisation processes and access control to the data residing in the different databases, service bastioning, backup policies, encryption of data in transit or at rest, auditing, etc. can be reviewed.

Regardless of the technology of the database product to be deployed (Oracle, DB2, SQL, SQL Server, etc.), several recommendations must be met to preserve the security of the information and integrity of the databases in the event of a hypothetical security incident.

Once the installation process has been carried out, which differs depending on the technology deployed, the following security recommendations grouped into different categories, depending on the scope of the platform where the service is running or the environment and capabilities provided by the database manager, should be carried out.

A number of recommendations must be complied with in order to preserve the security of the information and the integrity of the databases in the event of a hypothetical security incident.

3. Secure database implementation

During the installation process of the database, user identifiers, a group and a password are created and their values are usually implemented by default. In case the technology allows it, it will be necessary to modify them during the installation.

Database managers can use the operating system's own authentication mechanisms to identify and authenticate users. Therefore, it is highly recommended to specify strong authentication requirements at the operating system level.

It is also recommended to review and modify the default privileges that have been granted to users during installation. In turn, it is recommended to create instance-specific instance owner user IDs for each instance, adding it only as an instance owner group member and not using it in any other group. This allows greater control over the number of users and groups that can modify an instance.

Finally, during the installation of the database managers, it is recommended to use strong passwords that comply with the organisation's security policies. These characteristics are usually the usual ones when creating a password: use uppercase and lowercase letters, numbers, special characters and a certain length.

4. Secure database configuration

Information is an asset that must be protected through the **implementation of preventive measures that protect the integrity and confidentiality of data.** The safekeeping and handling of information should be considered as the backbone of a security strategy to reduce exposure to attacks and prevent possible unwanted data leakage.

4.1 Access control

Security measures focused on access to a resource **must be precise in access control and tailored to the needs of data exploitation** by users. As a result, the risk of unauthorised access and information leakage is considerably reduced.

With proper access control settings, you can determine which users have access to which data, and even which operations they can perform on that data.

Security and authorisation rules must be defined.

There must be a way to check **access requests by requested operations,** requested data and requesting users according to the applicable security rules.

- The system must be able to **recognise the origin of a user request** in order to decide which security rules are applicable to a certain request.
- The Database Administrator should be the figure **who can only perform the following actions:**
  - **Create user accounts** for database access.
  - **Grant and cancel privileges** to user accounts.
  - Assign user accounts to **security or accreditation levels.**

Authentication is the process by which a system verifies the identity of a user by means of authentication protocols such as LDAP, TNS, SSL, Kerberos, etc.

It is recommended to implement the necessary measures to delimit responsibility in each system when there are interconnected systems, where identification occurs in different security domains.

Authentication is the process by which a system verifies the identity of a user by means of authentication protocols such as LDAP, TNS, SSL, Kerberos, etc. Authentication mechanisms are based on **"something you know" such as passwords or agreed keys**, **"something you have" such as logical components** (certificates, OTP systems), **physical devices** (tokens) and **"something you are" such as biometric elements.**

The authentication factors used in the system shall be referred to as **credentials**. Before users possess authentication credentials, they shall be reliably identified in the system.

Access to an instance or a database requires user authentication. Depending on the database manager, authentication may be configured through the mechanisms enabled by the operating system, the database manager's own mechanisms, or a mixed configuration. In all cases, **it is recommended to ensure the access controls defined above.**

4.1.1 User account control

Default user accounts are **a clear vector of attack on any of the existing database solutions.** Therefore, they must meet certain security criteria to minimise their exposure and possible exploitation.

The **security of user accounts** must meet the following criteria:

- **Segregation of Privileges and Minimal Exposure.** Permissions should only be given to objects to which access should be granted.
- Special care must be taken with the **privileges granted,** ensuring that only those necessary are assigned.
- It is recommended to **create instance-specific instance owner user identifiers for each instance,** adding it only as a member of the group that owns the instance and not using it in any other group. This allows for more control over the number of users and groups that can modify the instance.
- The recommended **user account password security** guidelines are**:**
  - **Contain at least 12 characters.**
  - **Include capital letters, at least two.**
  - **Contain at least two lower case letters.**
  - **Contain at least two numbers.**
  - **Contain at least two special characters.**
  - **Do not contain the user's name.**
  - **Maximum lifetime of a password before forcing it to be changed 180 days.**
- **Account blocking.** Parameters must be configured to determine:
  - Number of failed login attempts allowed before the user account is locked.
  - Number of days an account will be blocked after a series of failed login attempts.
  - Set an active session time limit for all accounts on the application server.

- **Define a limited number of sessions** per user for non-database server accounts.
- **Set an inactivity logout time** for non-application server accounts.

- **Specific user accounts must be set up for the application servers.**

- **User accounts must be nominative in order to guarantee the traceability of the different actions executed in the engine.** Generic accounts associated with the different roles should not be used, but rather accounts that unequivocally identify the author of any change.

- It is desirable to have a **user certificate for each account** with access to the engine.

- **It is recommended to set up a two-factor authentication to the database engine for application server accounts,** with logins such as Google Authenticator or other social networks (Social Sign-In Authentication. This is recommended for application servers where an undetermined number of users will connect.

4.1.2 Roles and groups

During the creation of database objects, permissions can be granted on each object using precise instructions based on the principle of least privilege.

User accounts must be associated with types or roles. The minimum roles or account types defined by the manufacturer are:

Typical database users: They are usually restricted to their schema which contains their tables, views, indexes and stored procedures.

Application accounts: Used to run your own and third-party applications.

Application administrators: These accounts are used to administer, fix vulnerabilities and update the application. They must therefore have full access to all data and stored procedures used for the application.

Data analysts or business intelligence users: These users typically have unrestricted read access to the application schema without going through application-level access controls.

Database Administrators (DBAs): They are responsible for a wide variety of database tasks including performance management, diagnostics and tuning, updating and fixing vulnerabilities, database start-up and shutdown, and database backup. Your highly privileged database access also gives you access to any sensitive data contained in the database (personal records, health records, corporate financial records, etc.) although such access is not required to perform DBA tasks.

Security administrators: perform the responsibilities of security administrators, including user account management, encryption key management and audit management.

It is therefore recommended that:

- Review and modify default privileges granted to users during installation of the database manager.
- Under no circumstances should an account associated with both the **DBA** role and the Security Administration role be generated. Two different nominative accounts must be generated if the credentials of both roles must be given to the same natural person in order to improve the management of role segregation.
- User accounts assigned to application servers must not have quotas.
- It is recommended to revoke the privilege to create databases for all users except the **DBA** user.
- It is recommended to review, and, if necessary, revoke permissions of users or groups that do not need them, including **DBA** privileges.
- It is recommended to check that no public access has been granted to any database.
- It is recommended to control access to sensitive data at record, column, row or cell level **(RCAC and RLS)**.
- It is recommended to configure tag-based access control **(LBAC, RBAC).**

4.2 Audit

Auditing is a fundamental component in strengthening the security of an IT environment, especially in multi-user environments, where there is a need to know the actions performed by each of the users.

Monitoring of individual user and application access, including system administration actions, can provide a historical record of database system activity.

The audit function **allows auditing at instance level as well as at individual database level,** with all activities being recorded independently in separate logs for each.

Auditing is a fundamental component in strengthening the security of an IT environment.

- For each category, a**udit policies can be generated to record failures, successes or both.** It should be noted that enabling all categories and all events can lead to over-reporting and a high number of records.
- It is recommended to **review the audit event logging needs and to select only those events that are important** for the organisation or those that are related to the security of the system.
- It is recommended to **create an AUDITOR role and grant the necessary privileges** to read and manage audit events.
- It is recommended to **control access to the AUDITOR role through trusted contexts.** This allows restricting access only to connections originating from trusted computers.
- It is recommended that **the generated audit files should not be copied, modified or deleted directly** by the operating system administrator or by any other unauthorised user of the platform.
- It is recommended to **encrypt the authoring records stored on disk (data at rest),** both on the database server and on the log centraliser service, if one is available.

- It is recommended to **audit controlled access to the encryption key of the backups.**
- It is recommended to **audit all DBA actions.**
- It is recommended to **audit user access,** in particular those who have access to sensitive data.
- It is recommended to **audit all accesses to important tables.**
- It is recommended to **audit all database creation attempts.**
- It is recommended that **audit trails be integrated into a SIEM tool that allows real-time correlation of events,** analysis of data and provides the technical capability to investigate security incidents.

4.3 Measures to protect communications

Network security measures are the security controls that are added to protect the confidentiality, integrity and availability of information. The following are recommendations for measures to protect data in transit with the highest degree of reliability.

- Enable the use of **TLS 1.2** or higher and restrict the use of **SSL, TLS 1.0** or **TLS 1.1** on networks using **TCP/IP.**
- **Firewall** implementation and configuration.
- It is recommended to use **robust cipher algorithm** sets endorsed by the National Cryptologic Centre.
- It is recommended to **use certificates issued by a trusted certification authority.**

- It is recommended to **change the manufacturer's default ports.**
- The configuration of **IP whitelists and blacklists as well as ranges** with access to the server is recommended

The listener service monitors incoming network traffic and is one of the components most likely to be susceptible to distributed denial of service (DDoS) attacks. The components of this service must be secured and audited.

The following are recommendations on the security of the service:

- **Security measures must be applied to access to the service's files.**
- **Service access permissions should be reviewed.**
- It is recommended to **change the default name of the service files.**
- **The audit must be enabled.**
- It is recommended to **edit and change the manufacturer's default ports,** also modifying the permissions in the **firewall**.
- **SQL traffic between client and server** must be encrypted using secure algorithms. **Obsolete algorithms such as** DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 and RC4_256 **should be discarded.**

4.4 Information protection measures

Information protection measures include both those that are configured or implemented in the database server environment as well as in the operating system environment running the server.

4.4.1 Access control based on rows and columns

Row and column-based access control (RCAC) is an additional layer of security for controlling access to information in a table, column, row or cell. With this feature, the configuration of which depends on the manufacturer, you can ensure that information is adequately protected, ensuring that users only have access to the subset of data they require to perform their tasks.

A**dvantages of row and column-based access control:**

4. Secure database configuration

- Row and column-based access control complies with the **"need to know"** principle.
- **No database user is inherently exempt from row and column access control rules.**
- **Table data is protected regardless** of how a **table is accessed via SQL.**
- **Applications,** makeshift query tools and reporting tools **are all subject to row and column-based access rules.** The application is data-centric.

The row- and column-based security model focuses on **who accesses what information,** not on a static set of permissions. Result sets for the same query change depending on the context in which **the query was requested and no warnings or errors are returned.**

It is recommended to design and make use of row- and column-based access policies in environments where there are regulations or standards to comply with and access to data has to be made according to the context of the requester.

4.4.2 Tag-based access control

Label-based access control **(LBAC)** is a security model that is primarily intended for government applications or applications with known classification grades, as it requires data and users to be classified with a fixed set of rules that are implemented.

Tag-based access control allows control over who can access the data, increasing control over who can read or query and who can modify row and column information.

A tag-based security policy includes the following information:

- Which **security label components are used in the security** labels that are part of the policy.
- What **rules are used when comparing the components** of the security label.
- Which of **certain optional behaviours are used when accessing data** protected by the policy.
- **What additional security labels and exceptions should be considered when enforcing access to data protected by the security policy.**

Each protected table must have one and only one security policy associated with it. The rows and columns of that table can only be protected with security labels that are part of that security policy and all access to the protected data follows the rules of that policy.

You can have multiple security policies on a single database, but you cannot have more than one security policy protecting a given table.

It is recommended to use tag-based access control at the record level when **handling sensitive or classified information related to government entities.**

Tag-based access control at record level is recommended when the following statements are true:

- **The degree of classification of the data is known.**
- **The classification of data can be represented by one or more security labels.**
- **Authorisation rules can be linked to the components of the security label.**

Access control based on column level labels is recommended when:

- **Sensitive columns need to be protected from unauthorised access by the table owners or even the DBA.**

  It is required to protect entire tables from unauthorised access to the table owners or even the DBA. In this case, you will assign a security label to all columns of the table, then assign the security label to a role and assign that role only to users who require access to the table information.

Regardless of the access controls implemented, it is recommended to make use of encryption at rest mechanisms for data, tables, audit files and backup files at the operating system level.

4.4.3 Dynamic data masking

Information masking is a **feature that anonymises and hides data,** limiting unprivileged users' access to the most sensitive information.

With data masking, **sensitive information can be hidden from the result set obtained** from a query of designated fields in a database.

It is possible to define masking rules on a column in a table in order to obfuscate the data in that column. However, creating a mask on a column does not prevent updates to the column. Therefore, **it is necessary to have an appropriate access control policy or policy** to limit update permissions.

4.4.4 Backup policies

A backup is a **process by which existing information is duplicated from one medium to another, in order to be able to recover it in case of failure of the first data host.**

Sometimes, a poor backup protection policy allows unauthorised access to information. Therefore, if data is protected by backups, it can be accessed directly from the backup service of any database manager.

The following general good practices are set out below, regardless of the product version.

It is recommended to **encrypt all backup files and archive images,** regardless of the medium on which they are stored.

It is recommended to ensure that the **restoration of any backup should require controlled access to the encryption key and should be audited,** both the access and the restoration itself.

The manufacturer's recommended backup practices should be maintained.

Regular backups are recommended. At least one incremental backup should be generated daily and kept for **seven days**. A weekly incremental backup should also be generated on Sunday and kept for four weeks. In addition, an incremental copy must be generated every first day of the month with the last twelve months retained. Finally, **an annual backup must be generated and retained for five years.**

Store backups in locations other than the physical location of the production server.

It is recommended to **store backups on redundant disk systems.**

Conduct regular recovery tests in the form of a dry run.

4.4.5 Encryption

Encryption is the conversion of data available in a readable format into another encoded format creating the need to decrypt it in order to process it. Encryption involves using a cryptographic key that is generated by mathematical values agreed upon by both the sender and receiver to convert the content of a message into an unreadable format, allowing the information to be protected from external and unauthorised agents.

It is the responsibility of the organisation to know and secure the most sensitive data in its possession. This depends on the content of the information in the various databases. Not all data has the same criticality and it is up to the organisation to first categorise the information, and then secure access to it according to the sensitivity of the data.

Different encryption protocols are available depending on the state of the information. Thus, encryption can be categorised as follows:

Encryption in transit: Data is considered to be in transit when it is moved between devices. During the transfer of information, data is at increased risk due to the need to decrypt before transferring.

Encryption of data during transfer is known as end-to-end encryption. End-to-end encryption ensures that data privacy is protected, even if the data is intercepted. It is recommended to use encryption protocols for SQL traffic between clients and servers such as AES, FIPS, Triple DES, TLS, etc.

Encryption at rest: data at rest is considered to be data at rest when it is collected and stored on hard drives, backup tapes or in the cloud, it is considered to be inactive and stable. Data at rest should always be encrypted and can be encrypted using protocols such as AES, Triple DES, SHA, etc.

In addition, encryption of the entire database, database objects, tables, columns, cells, audit trails and all backups is recommended, regardless of the medium on which they are stored.

The National Cryptologic Centre has specific configuration guides that contain the details of Database Encryption among other relevant information for Oracle and DB2 databases.

- Security recommendations for Oracle database 19C.
- Security recommendations for DB2 databases.

4.5 Software review

After installation of the product and its updates, the status of the solution must be checked. The permissions of already secured objects may have changed and should be checked again.

It is important to review the documentation of the affected objects and review them afterwards. At the software level, the following maintenance tasks should be performed on a regular basis:

- **Keep the engine version up to date.**
- Keep versions of any engine-dependent software up to date.
- It is recommended to configure **alarms for consumption and use of the DB engine.**
- It is recommended to **document all changes to the DB engine and administration tasks.**
- Verify that **user accounts are not root** in the operating system.
- **Review the vulnerabilities of each component belonging to the installation.** Known vulnerabilities (CVEs) per component (CPE) can be consulted on portals such as NIST.
- In case vulnerabilities are published and have not been corrected by the manufacturer, **they should be reported to senior security officers.**
- **Clean up temporary files** after product installation, upgrade or vulnerability fixes.

5. Glossary

TLS: Transport Layer Security is a communications protocol whose main purpose is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS registration protocol and the TLS handshake protocol. During TLS negotiation, a public key algorithm is used to securely exchange digital signatures and encryption keys between a client and a server. The identity information and the key are used to establish a secure connection for the session between the client and the server. Once the secure session is established, the data transmission between the client and the server is encrypted using a symmetric algorithm, such as AES.

RCAC: Row and Column Access Control. It allows access to a table to be controlled at row level, column level or both and can be used to complement the table privilege model, ensuring that information is adequately protected and that users only have access to the subset of data that is required to perform their job tasks and comply with specific rules and regulations.

LBAC: Label Based Access Control. It is a security model that is primarily intended for government applications or applications with known classification grades, as it requires data and users to be classified with a fixed set of rules that are implemented.

DBA: Database Administrator.

FIPS: Federal Information Processing Standards. Federal Information Processing Standards (FIPS) Publication 140-2 is a U.S. government standard that defines the minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

LDAP: Lightweight Directory Access Protocol refers to an application-level protocol, which allows access to an ordered and distributed directory service to search for information in a network environment.

5. Glossary

SSL: Secure Sockets Layer, the standard technology for keeping an Internet connection secure, as well as for protecting any sensitive information sent between two systems and preventing criminals from reading and modifying any data being transferred, including information that could be considered personal.

Kerberos: It is a computer network authentication protocol created by MIT that allows two computers on an insecure network to prove their identity to each other in a secure manner.

OTP: One-time password used for authentication.

Social Sign-In Authentication: Social Sign-In is a single sign-on for end users. With existing login information from a social media provider such as Facebook, Twitter or Google, the user can log in to a third-party website instead of creating a new account specifically for that website.

AES: Advanced Encryption Standard (AES), is a block cipher scheme adopted as an encryption standard by the United States government, created in Belgium. AES was announced by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197 (FIPS 197) on 26 November 2001 after a 5-year standardisation process. It became an effective standard on 26 May 2002. Since 2006, AES is one of the most popular algorithms used in symmetric cryptography.

DES: Data Encryption Standard (DES) is an encryption algorithm, i.e. a method for encrypting information, chosen as a FIPS standard in the United States in 1976, and whose use has spread widely around the world.

Triple DES: In cryptography, Triple DES is the name given to the algorithm that does triple DES encryption.

SHA: Secure Hash Algorithms1 are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a US Federal Information Processing Standard (FIPS).

5. Glossary

SIEM: Security Information and Event Management (SIEM) is a cyber security term where services and software products combine two systems: Security Information Management (SIM) and Security Event Management (SEM).

DDoS: In computer security, a denial of service attack, also called a DoS (Denial of Service) attack, is an attack on a computer system or network that causes a service or resource to be inaccessible to legitimate users.

CVE: Common Vulnerabilities and Exposures (CVE) is a list of recorded information on known security vulnerabilities, in which each reference has a CVE-ID number, description of the vulnerability, which versions of the software are affected, possible workaround (if any) or how to configure to mitigate the vulnerability and references to publications or forum or blog posts where the vulnerability has been made public or its exploitation is demonstrated. In addition, a direct link to information from the NIST Vulnerability Database (NVD), where more details of the vulnerability and its assessment can be obtained, is usually also displayed.

NIST: The National Institute of Standards and Technology (NIST), called the National Bureau of Standards (NBS) between 1901 and 1988, is an agency of the Technology Administration of the U.S. Department of Commerce. The mission of this institute is to promote innovation and industrial competition in the United States through advances in metrology, standards and technology in ways that enhance economic stability.

RLS: Row-Level Security. Row-level security allows you to use group membership or execution context to control access to rows in a database table.

6. Summary table of security enhancement measures

FIELD	NUM	MEASURE	MOTIVE
SECURE IMPLEMENTATION	1	On Unix or Linux systems, it is recommended to specify different usernames than those created by default, regardless of the database manager to be implemented.	Avoid using default names to plan attacks on the database.
	2	On Windows systems, it is recommended to change this default setting and specify different user names for each role.	Avoid using default names to plan attacks on the database.
	3	It is recommended to create instance-specific instance owner user IDs for each instance, adding it only as a member of the instance owner group and not using it in any other group.	Have more control over the number of users and groups that can modify the instance.
	4	During installation, it is recommended to use strong passwords that comply with the organisation's security policies.	Minimise the possibility of brute force attacks.
ACCESS CONTROL	5	We recommend the use of strong and strong passwords containing at least 12 characters, including uppercase, lowercase, numbers and special characters.	Minimise the possibility of brute force attacks.
	6	It is recommended to set the maximum lifetime of a password to no more than 180 days.	Time limits the attacker to compromise a user's password.
	7	It is recommended to set up account blocking policies.	Limit an attacker's attempts to access system resources.
	8	It is recommended to set up specific user accounts for the application servers.	Limit the attack surface.
	9	It is advisable to establish a two-factor authentication.	Increasing the security of users' digital identity.

6. Summary table of security enhancement measures

FIELD	NUM	MEASURE	MOTIVE
ACCESS CONTROL	10	It is recommended to make use of strong authentication and communication mechanisms such as SERVER, LDAP TLS or Kerberos.	Improve the security and reliability of authentication mechanisms.
	11	It is recommended to follow the principle of least privilege, where only users are allowed to access the information and do the actions they really need.	Minimise the exposure surface.
	12	It is recommended to review and, if necessary, revoke permissions of users or groups that do not need them.	Minimise the exposure surface.
	13	In scenarios where sensitive data is stored, it is recommended, in addition to reviewing privileges, to establish granular access controls.	Prevent access to sensitive roles from untrusted environments.
	14	It is recommended to revoke the DBA's data access privileges if he/she has no real need to access the data.	By default, a DBA has access to any table in his or her database instance. This poses a risk, especially if the account has been breached or if these privileges are abused.
	15	It is recommended to check that no public access has been granted to any database.	Minimise the exposure surface.
	16	It is recommended to assign privileges through a role model, avoiding direct assignment to users.	Improve control and maintenance of access privileges.
	17	It is recommended to use the access controls of the operating system.	Prevent operating system administrators from gaining too much access.
	18	It is recommended to assign DBA permissions only through a role, and to control access to this role through trust contexts.	Allows to restrict access only to connections originating from trusted computers.
	19	It is recommended to revoke the privilege to create databases for all users except the DBA.	Minimise the exposure surface.
AUDIT	20	It is recommended to review the audit event logging needs and to select only those events that are important for the organisation or those that are related to the security of the system.	Control the audit information generated, avoiding irrelevant data and storage problems that may lead to loss of relevant evidence.
	21	It is recommended to create an AUDITOR role and grant the necessary privileges to read and manage audit events.	Control who can access audit information and how.

6. Summary table of security enhancement measures

FIELD	NUM	MEASURE	MOTIVE
AUDIT	22	It is recommended to control access to the AUDITOR role through trusted contexts.	Allows to restrict access only to connections originating from trusted computers.
	23	It is recommended that the generated audit files should not be copied, modified or deleted directly by the operating system administrator or by any other unauthorised user of the platform.	Prevent exfiltration of data or access to sensitive audit information by bypassing database security mechanisms.
	24	It is recommended to make use of a centralising service (SIEM) for audit trails.	Unification of different audit sources, facilitating log correlation and avoiding loss or manipulation of evidence.
	25	It is recommended to encrypt the authoring records stored on disk (data at rest), both on the database server and on the log centraliser service, if one is available.	Prevent exfiltration of data or access to sensitive audit information by bypassing database security mechanisms.
	26	It is recommended to audit all DBA actions.	Maintain an audit trail of administrative actions that may compromise the system.
	27	It is recommended to audit user access, in particular those who have access to sensitive data.	Maintain an audit trail of user actions.
	28	It is recommended to audit all accesses to important tables.	Maintain an audit trail of actions that may compromise the system.
	29	It is recommended to audit all attempts to create databases.	Maintain an audit trail of administrative actions that may compromise the system.
	30	It is recommended to audit controlled access to the encryption key of the backups.	Maintain an audit trail of actions that may compromise information.
COMMUNICATIONS PROTECTION	31	It is recommended to make use of encryption with secure algorithms exposed at the communications layer, such as TLS 1.2 or higher.	Prevent data capture in transit through the network.
	32	It is recommended not to encrypt data using obsolete algorithms.	The following algorithms are deprecated: DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 and RC4_256 and should not be used.

6. Summary table of security enhancement measures

FIELD	NUM	MEASURE	MOTIVE
COMMUNICATIONS PROTECTION	33	It is recommended to use robust cipher algorithm sets endorsed by the National Cryptologic Centre.	Prevent exploitation of vulnerabilities in weak or obsolete algorithms.
	34	Firewall implementation and configuration.	Increase control of traffic in and out of ports.
	35	It is recommended to change the manufacturer's default ports.	Increase access security.
	36	It is recommended to review and configure the ports used by all server instances.	Minimise the exposure surface, enabling only the necessary communication ports.
PROTECTION OF INFORMATION	37	It is recommended to design and make use of granular access policies to records, columns or rows in environments where there are regulations or standards to comply with and access to data has to be made according to the context of the requester.	Comply with the "need to know" principle.
	38	It is recommended to make use of tag-based access control at the record level when handling sensitive or classified information related to government entities.	Comply with the "need to know" principle.
	39	It is recommended to use tag-based access control at record level when the following statements are true: – The degree of classification of the data is known. – The classification of data can be represented by one or more security labels. – Authorisation rules can be linked to the components of the security label.	Comply with the "need to know" principle.
	40	Access control based on column level labels is recommended when: – It is required to protect sensitive columns from unauthorised access to the table owners or even the DBA. – It is required to protect entire tables from unauthorised access to the table owners or even the DBA.	Comply with the "need to know" principle.
	41	It is recommended to limit the exposure of sensitive information by hiding it from unprivileged users through dynamic data masking. The availability of this feature depends on the manufacturer.	Comply with the "need to know" principle.

6. Summary table of security enhancement measures

FIELD	NUM	MEASURE	MOTIVE
BACKUP	42	It is recommended to encrypt all backup files and archive images, regardless of the medium on which they are stored.	Prevent unauthorised access to backups.
	43	It is recommended to ensure that the restoration of any backup should require controlled access to the encryption key and should be audited, both the access and the restoration itself.	Prevent unauthorised access to backups and log any access through auditing.
	44	Store backups at locations other than the physical location of the production server.	Avoid unavailability of information in case of attack or system failure.
CIFRED	45	Encryption of the entire database, database objects, tables, columns, cells, audit trails and all backups is recommended, regardless of the medium on which they are stored.	Protect privacy.
SOFTWARE REVIEW	46	It is recommended to keep the engine version up to date and the software dependent.	Fix vulnerabilities that may affect the database.
	47	The configuration of consumption alarms and use of the database engine is recommended.	Monitoring system resources prevents errors that may affect access to data.

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es