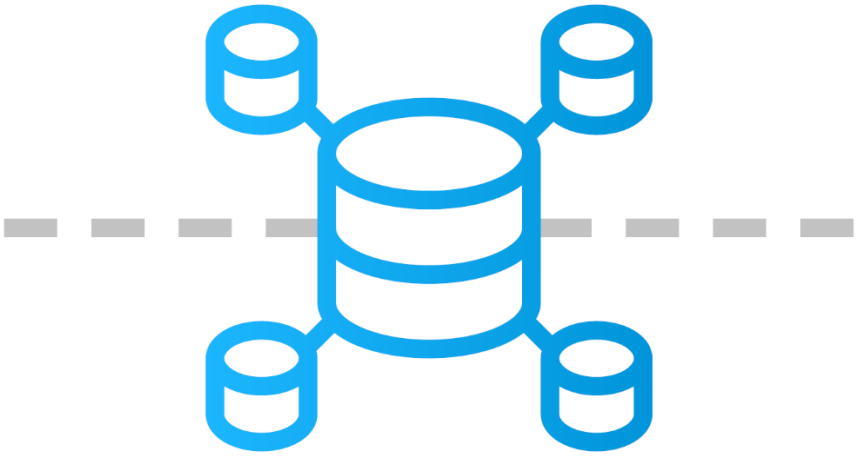
CCN
centro criptológico nacional

CCN-CERT BP/24

RECOMENDACIONES DE SEGURIDAD EN BASES DE DATOS



DICIEMBRE 2021

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.12.23 15:13:46 +01'00'

P.º de la Castellana 109, 28046 Madrid

Fecha de Edición: octubre de 2021
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

diciembre de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. FUNDAMENTOS DE LA SEGURIDAD DE LAS BASES DE DATOS

Uno de los principales objetivos de ataque suele ser las bases de datos porque albergan información sensible. Es recomendable la implantación de una serie de directrices de seguridad manteniendo el cumplimiento de la legislación en materia de seguridad y privacidad.

Los sistemas gestores de bases de datos se ejecutan sobre plataformas específicas y sistemas operativos que les proporcionan los elementos fundamentales de comunicación y de acceso.

El modelo de seguridad de un sistema gestor de bases de datos estará dividido en dos ámbitos de actuación:

a) El ámbito de la plataforma donde se ejecuta el servicio.

b) El entorno y las capacidades que proporciona el propio gestor de bases de datos.

En el ámbito de la plataforma donde se ejecuta el servicio se pueden revisar los aspectos de seguridad que se configuran en el ámbito del sistema operativo, como usuarios, servicios, comunicaciones y protocolos.

Por otro lado, en el entorno y capacidades que proporciona el gestor de base de datos pueden revisarse aspectos como procesos de autorización y control de acceso a los datos que residen en las distintas bases de datos, bastionado de servicios, políticas de Backup, cifrado de los datos en tránsito o reposo, auditoría, etc.

Independientemente de la tecnología del producto de Base de Datos que se vaya a desplegar (Oracle, DB2, SQL, SQL Server, etc.), deben cumplirse una serie de recomendaciones para preservar la seguridad de la información y la integridad en las Bases de Datos ante un hipotético incidente de seguridad.

Una vez llevado a cabo el proceso de instalación, el cual es diferente en función de la tecnología desplegada, se deben llevar a cabo las siguientes recomendaciones de seguridad agrupadas en diferentes categorías, según el ámbito de la plataforma donde se ejecuta el servicio o bien el entorno y las capacidades proporcionadas por el gestor de bases de datos.

3. IMPLEMENTACIÓN SEGURA DE LA BASE DE DATOS

Durante el proceso de instalación de la base de datos se crean identificadores de usuario, un grupo y una contraseña cuyos valores suelen venir implementados por defecto. En caso de que la tecnología lo permita será necesario modificarlos durante la instalación.

Los gestores de base datos pueden utilizar los mecanismos de autenticación propios del sistema operativo para identificar y autenticar a los usuarios. Por ello, es muy recomendable especificar requisitos robustos de autenticación a nivel del sistema operativo.

También es recomendable revisar y modificar los privilegios predeterminados que se han otorgado a los usuarios durante la instalación. A su vez, se recomienda crear identificadores de usuarios propietarios de instancias específicos para cada instancia, añadiéndolo solo como miembro de grupo propietario de la instancia y no usarlo en ningún otro grupo. Esto permite un mayor control en el número de usuarios y grupos que pueden modificar una instancia.

Finalmente, durante la instalación de los gestores de bases de datos, se recomienda hacer uso de contraseñas robustas que cumplan las directivas de seguridad de la organización. Estas características suelen ser las habituales al crear una contraseña: hacer uso de mayúsculas y minúsculas, números, caracteres especiales y una longitud determinada.

4. CONFIGURACIÓN SEGURA DE LA BASE DE DATOS

La información es un activo que debe protegerse mediante la implantación de medidas preventivas que protege la integridad y confidencialidad de los datos. La custodia y el manejo de la información debe considerarse como el eje principal de una estrategia de seguridad para reducir la exposición a ataques y evitar las posibles fugas indeseadas de los datos.

4.1 CONTROL DE ACCESO

Las medidas de seguridad centradas en el acceso a un recurso deben ser precisas en el control de acceso y ajustadas a las necesidades de explotación de los datos por parte de los usuarios. Gracias a ello, el riesgo de sufrir accesos no autorizados y fugas de información se reduce considerablemente.

Con una adecuada configuración de control de acceso, se puede determinar qué usuarios tienen acceso a qué datos, e incluso qué operaciones pueden realizar sobre dichos datos.

a) Se deben definir reglas de seguridad y autorización.

b) Debe existir una forma de comprobar las peticiones de acceso mediante operaciones solicitadas, datos solicitados y usuarios solicitantes según las reglas de seguridad aplicables.

c) El Sistema debe ser capaz de reconocer el origen de una petición usuario para decidir qué reglas de seguridad son aplicables a cierta petición.

d) El Administrador de la Base de Datos, debe ser la figura que únicamente pueda realizar las siguientes acciones:

   i. Crear cuentas de usuario para acceso a la base de datos.

   ii. Conceder y cancelar privilegios a las cuentas de usuarios.

   iii. Asignar cuentas de usuario a niveles de seguridad o acreditación.

Se recomienda aplicar las medidas necesarias para delimitar la responsabilidad en cada sistema cuando existan sistemas interconectados, donde la identificación se produzca en diferentes dominios de seguridad.

La autenticación es el proceso por el cual un sistema verifica la identidad de un usuario mediante protocolos de autenticación como LDAP, TNS, SSL, Kerberos, etc. Los mecanismos de autenticación se basan en “algo que se sabe” como contraseñas o claves concertadas, “algo que se tiene” como componentes lógicos (certificados, Sistemas OTP), dispositivos físicos (tokens) y “algo que se es” como elementos biométricos.

Los factores de autenticación que se utilizan en el sistema se denominarán credenciales. Antes de que los usuarios posean las credenciales de autenticación, éstos deberán haberse identificado de manera fidedigna en el sistema.

El acceso a una instancia o una base de datos requiere que el usuario se autentique. Dependiendo del gestor de base de datos, la autenticación podrá configurarse a través de los mecanismos habilitados por el sistema operativo, de los mecanismos propios del gestor de la base de datos o bien mediante una configuración mixta. En cualquiera de los casos se recomienda garantizar los controles de acceso definidos anteriormente.

4.1.1 CONTROL DE CUENTAS DE USUARIOS

Las cuentas predeterminadas de usuario son un claro vector de ataque sobre cualquiera de las soluciones de bases de datos existentes. Por ello, éstas deben cumplir unos criterios de seguridad para minimizar su exposición y posible explotación.

La seguridad de las cuentas de usuario debe cumplir los siguientes criterios:

a) Segregación de Privilegios y Mínima Exposición. Solo se deben dar permisos a los objetos a los que se deba tener acceso.

b) Se debe tener especial cuidado con los privilegios concedidos, asegurando que únicamente se asignan los necesarios.

c) Se recomienda crear identificadores de usuarios propietarios de instancias específicos para cada instancia, añadiéndolo solo como miembro del grupo propietario de la instancia y no usarlo en ningún otro grupo. Esto permite disponer de un mayor control en el número de usuarios y grupos que pueden modificar la instancia.

d) Las pautas de seguridad de contraseñas de las cuentas de usuario recomendadas son:
   i. Contener al menos 12 caracteres.
   ii. Incluir mayúsculas, al menos dos.
   iii. Contener al menos dos minúsculas.
   iv. Contener al menos dos números.
   v. Contener al menos dos caracteres especiales.
   vi. No contener el nombre del usuario.
   vii. Tiempo máximo de vida de una contraseña antes de forzar a cambiarla 180 días.

e) Bloqueo de cuentas. Se deben configurar parámetros que determinen:
   i. Número de intentos fallidos de inicio de sesión permitidos antes de que se bloquee la cuenta de usuario.
   ii. Número de días que se bloqueará una cuenta después de una serie de intentos fallidos de inicio de sesión.
   iii. Establecer un límite de tiempo de sesión activo para todas las cuentas del servidor de aplicaciones.
   iv. Definir un número limitado de sesiones por usuario para cuentas no pertenecientes al servidor de bases de datos.
   v. Establecer un tiempo de cierre de sesión por inactividad para cuentas no pertenecientes al servidor de aplicación.

f) Se debe configurar cuentas de usuario específicas para los servidores de aplicaciones.

g) Las cuentas de usuarios deben ser nominativas para poder garantizar la trazabilidad de las distintas acciones ejecutadas en el motor. No deben usarse cuentas genéricas asociadas a los distintos roles sino cuentas que identifiquen inequívocamente al autor de cualquier cambio.

h) Es conveniente disponer un certificado de usuario para cada cuenta con acceso al motor.

i) Es recomendable establecer un doble factor de autentificación al motor de base de datos para las cuentas de servidor de aplicación, con accesos como Google Authenticator u otras redes sociales (Social Sign-In Authentication). esto es recomendable para los servidores de aplicaciones donde se van a conectar un número indeterminado de usuarios.

4.1.2 ROLES Y GRUPOS

Durante la creación de objetos de base de datos, puede concederse permisos en cada objeto usando instrucciones precisas basadas en el principio de menor privilegio.

Las cuentas de usuarios deben asociarse a tipos o roles. Los roles o tipos de cuentas definidos por el fabricante como mínimo son:

a) **Usuarios habituales de bases de datos:** Normalmente están restringidos a su esquema las cuales contienen sus tablas, vistas, índices y procedimientos almacenados.

b) **Cuentas de aplicaciones:** se utilizan para ejecutar las aplicaciones propias y de terceros.

c) **Administradores de aplicaciones:** Estas cuentas se utilizan para administrar, corregir vulnerabilidades y actualizar la aplicación. Por tanto, deben tener acceso completo a todos los datos y los procedimientos almacenados utilizados para la aplicación.

d) **Analistas de datos o usuarios de inteligencia empresarial:** Estos usuarios suelen tener acceso de lectura sin restricciones al esquema de aplicación sin pasar por los controles de acceso a nivel de aplicación.

e) **Administradores de bases de datos (DBA):** Son responsables de una amplia variedad de tareas para la base de datos incluida la gestión del rendimiento, el diagnóstico y el ajuste, la actualización y la corrección de vulnerabilidades, el inicio de la base de datos y apagado, y respaldo de la base de datos. Su acceso a la base de datos altamente privilegiado también le da acceso a cualquier dato confidencial contenidos en la base de datos (registros personales, de salud, de finanzas corporativas, etc.) aunque ese acceso no es necesario para realizar tareas de DBA.

f) **Administradores de seguridad:** realizan las responsabilidades de administradores de seguridad, incluida la gestión de cuentas de usuario, la gestión de claves de cifrado y gestión de auditoría.

Por ello, se recomienda:

a) Revisar y modificar privilegios predeterminados otorgados a los usuarios durante la instalación del gestor de base de datos.

b) Que en ningún caso se genere una cuenta asociada a la vez al rol DBA y al rol de Administración de Seguridad. Se debe generar dos cuentas nominativas distintas si debe entregar las credenciales de ambos roles a una misma persona física para mejorar la gestión de la segregación de roles.

c) Las cuentas de usuarios asignadas a servidores de aplicaciones no deben tener cuotas.

d) Se recomienda revocar el privilegio de crear bases de datos a todos los usuarios, excepto el usuario DBA.

e) Se recomienda revisar, y si es necesario revocar, aquellos permisos de usuarios o grupos que no los necesitan, incluido los privilegios del DBA.

f) Se recomienda comprobar que no se ha otorgado ningún tipo de acceso público a ninguna base de datos.

g) Se recomienda controlar el acceso a los datos sensibles a nivel de registro, columna, fila o celda (RCAC y RLS).

h) Se recomienda configurar el control de acceso basado en etiquetas (LBAC, RBAC).

4.2 AUDITORÍA

La auditoría es un componente fundamental en el refuerzo de la seguridad de un entorno informático, especialmente en entornos multi usuario, donde existe una necesidad de conocer las acciones realizadas por cada uno de los usuarios.

La supervisión del acceso de usuarios individuales y de aplicaciones incluidas las acciones de administración del sistema, puede proporcionar un registro histórico de la actividad de los sistemas de base de datos.

La función de auditoría permite auditar tanto a nivel de instancia como a nivel de base de datos individual, registrando de forma independiente todas las actividades en registros separados para cada una.

a) Para cada categoría, se pueden generar directivas de auditoría que registren los fallos, los aciertos o ambos. Hay que tener en cuenta que habilitar todas las categorías y todos los eventos puede provocar un exceso de información y un elevado número de registros.

b) Se recomienda revisar las necesidades de registro de eventos de auditoría y seleccionar únicamente aquellos eventos importantes para la organización o los que estén relacionados con la seguridad del sistema.

c) Se recomienda crear un rol AUDITOR y otorgar los privilegios necesarios para leer y administrar los eventos de auditoría.

d) Se recomienda controlar el acceso al rol AUDITOR mediante contextos de confianza. Esto permite restringir el acceso únicamente a conexiones originadas desde equipos de confianza.

e) Se recomienda evitar que los ficheros de auditoría generados puedan ser copiados, modificados o eliminados directamente por el administrador del sistema operativo o por otro usuario no autorizado de la plataforma.

f) Se recomienda cifrar los registros de autoría almacenados en el disco (datos en reposo), tanto en el servidor de bases de datos, como en el servicio centralizador de registros, en caso de disponer de uno.

g) Se recomienda auditar el acceso controlado a la clave de cifrado de las copias de seguridad.

h) Se recomienda auditar todas las acciones del DBA.

i) Se recomienda auditar el acceso de los usuarios, en particular aquellos que tengan acceso a los datos sensibles.

j) Se recomienda auditar todos los accesos a las tablas importantes.

k) Se recomienda auditar todos los intentos de creación de bases de datos.

l) Se recomienda que los registros de auditoría sean integrados en una herramienta SIEM que permita correlacionar eventos en tiempo real, analizar datos y otorgue la capacidad técnica para investigar incidentes de seguridad.

4.3 MEDIDAS DE PROTECCIÓN DE LAS COMUNICACIONES

Las medidas de seguridad de red son los controles de seguridad que se añaden para proteger la confidencialidad, integridad y la disponibilidad de la información. A continuación, se indican las recomendaciones de medidas para proteger con el mayor grado de confiabilidad los datos en tránsito.

a) Habilitar el uso de TLS 1.2 o superior y restringir el uso de SSL, TLS 1.0 o TLS 1.1 en las redes que utilicen TCP/IP.

b) Implantación y configuración del firewall.

c) Se recomienda utilizar conjuntos de algoritmos de cifrado robustos avalados por el Centro Criptológico Nacional.

d) Se recomienda hacer uso de certificados emitidos por una entidad de certificación de confianza.

e) Se recomienda cambiar los puertos por defecto del fabricante.

f) Se recomienda la configuración de listas blancas y negras de IPs así como rangos con acceso al servidor.

El servicio de agente de escucha o listener controla el tráfico de red entrante y es uno de los componentes con mayor probabilidad de ser susceptible a ataques de denegación de servicio distribuido (DDoS). Los componentes de este servicio deben estar asegurados y auditados.

A continuación, se exponen una serie de recomendaciones sobre la seguridad del servicio:

a) Se debe aplicar medidas de seguridad sobre los accesos a los ficheros del servicio.

b) Se debe revisar los permisos de acceso al servicio.

c) Se recomienda cambiar el nombre por defecto de los ficheros del servicio.

d) Se debe habilitar la auditoría.

e) Se recomienda editar y cambiar los puertos por defecto del fabricante, modificando también los permisos en el firewall.

f) Se debe cifrar el tráfico SQL entre clientes y servidor mediante algoritmos seguros. Deben descartarse los algoritmos obsoletos como DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 y RC4_256.

4.4 MEDIDAS DE PROTECCIÓN DE INFORMACIÓN

Las medidas de protección de la información incluyen tanto aquellas que se configuran o implementan en el entorno del servidor de bases de datos, como en el entorno del sistema operativo que ejecuta el servidor.

4.4.1 CONTROL DE ACCESO BASADO EN FILAS Y COLUMNAS

El control de acceso basado en filas y columnas (RCAC) es una capa adicional de seguridad para el control de acceso a la información de una tabla, columna, fila o celda. Con esta característica, cuya configuración depende del fabricante, se puede garantizar que la información esté protegida adecuadamente, garantizando que los usuarios solamente tengan acceso al subconjunto de datos que requieren para realizar sus tareas.

Ventajas del control de acceso basado en filas y columnas:

a) El control de acceso basado en filas y columnas cumple con el principio de “necesidad de conocer”.

b) Ningún usuario de la base de datos está inherentemente exento de las reglas de control de acceso a filas y columnas.

c) Los datos de la tabla están protegidos independientemente de cómo se acceda a una tabla a través de SQL.

d) Las aplicaciones, las herramientas de consulta improvisadas y las herramientas de generación de informes están todas sujetas a las reglas de acceso basado en filas y columnas. La aplicación está centrada en los datos.

El modelo de seguridad basado en filas y columnas se centra en quién accede y a qué información, no en un conjunto estático de permisos. Los conjuntos de resultados para la misma consulta cambian según el contexto en el que se solicitó la consulta y no se devuelve ninguna advertencia o error.

Se recomienda diseñar y hacer uso de políticas de acceso basado en filas y columnas en aquellos entornos donde existan una regulaciones o normativas que cumplir y el acceso a los datos tenga que realizarse según el contexto de quien lo solicita.

4.4.2 CONTROL DE ACCESO BASADO EN ETIQUETAS

El control de acceso basado en etiquetas (LBAC) es un modelo de seguridad que está destinado principalmente a aplicaciones gubernamentales o con grados de clasificación conocidos, ya que requiere que los datos y los usuarios se clasifiquen con un conjunto fijo de reglas que se implementan.

El control de acceso basado en etiquetas permite tener el control sobre quién puede acceder a los datos, aumentando el control sobre quién puede leer o consultar y quién puede modificar la información de las filas y columnas.

Una política de seguridad basada en etiquetas incluye la siguiente información:

a) Qué componentes de la etiqueta de seguridad se utilizan en las etiquetas de seguridad que forman parte de la política.

b) Qué reglas se utilizan al comparar los componentes de la etiqueta de seguridad.

c) Cuáles de ciertos comportamientos opcionales se utilizan al acceder a los datos protegidos por la política.

d) Qué etiquetas de seguridad adicionales y excepciones se deben considerar al hacer cumplir el acceso a los datos protegidos por la política de seguridad.

Cada tabla protegida debe tener una y solo una política de seguridad asociada. Las filas y columnas de esa tabla solo se pueden proteger con etiquetas de seguridad que forman parte de dicha política de seguridad y todo acceso a los datos protegidos sigue las reglas de dicha política.

Se pueden tener varias políticas de seguridad en una sola base de datos, pero no se puede tener más de una política de seguridad que proteja una tabla determinada.

Se recomienda usar el control de acceso basado en etiquetas a nivel de registros cuando se maneje información sensible o clasificada relacionada con entidades del gobierno.

Se recomienda el control de acceso basado en etiquetas a nivel de registros cuando las siguientes afirmaciones son ciertas:

a) Se conoce el grado de clasificación de los datos.

b) La clasificación de los datos se puede representar por una o varias etiquetas de seguridad.

c) Las reglas de autorización se pueden enlazar a los componentes de la etiqueta de seguridad.

Se recomienda el control de acceso basado en etiquetas a nivel de columna cuando:

a) Se requiera proteger columnas sensibles de accesos no autorizados a los dueños de la tabla o incluso al DBA.

b) Se requiere proteger tablas completas de accesos no autorizados a los dueños de la tabla o incluso al DBA. En este caso, se asignará una etiqueta de seguridad todas las columnas de la tabla, posteriormente se deberá asignar la etiqueta de seguridad a un rol y asignar dicho rol únicamente a los usuarios que requieren acceso a la información de la tabla.

Independientemente de los controles de acceso que se implementen, se recomienda hacer uso de mecanismos de cifrado en reposo de los datos, tablas, ficheros de auditoría y archivos de respaldo a nivel del sistema operativo.

4.4.3 ENMASCARAMIENTO DE DATOS DINÁMICOS

El enmascaramiento de la información es una característica que anonimiza y oculta los datos, limitando el acceso a los usuarios sin privilegios a la información más sensible.

Gracias al enmascaramiento de datos, se puede ocultar la información confidencial del conjunto de resultados obtenidos de una consulta de campos designados de una base de datos.

Es posible definir reglas de enmascaramiento en una columna de una tabla con el objetivo de ofuscar los datos de esa columna. Sin embargo, la creación de una máscara en una columna no impide que se efectúen actualizaciones en ella. Por tanto, es necesario disponer de una directiva o política de control de acceso adecuada para limitar los permisos de actualización.

4.4.4 POLÍTICAS DE BACKUP

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.

En ocasiones, una política de protección de copias de seguridad deficiente permite el acceso no autorizado a la información. Por ello, si los datos son protegidos mediante copias de seguridad pueden ser accesibles directamente desde el servicio de buckup de cualquier gestor de base de datos.

A continuación, se exponen las siguientes buenas prácticas generales independientemente de la versión del producto.

a) Se recomienda cifrar todos los ficheros de backup e imágenes de archivo, independientemente del medio donde se almacenen.

b) Se recomienda garantizar que la restauración de cualquier copia de seguridad debe requerir un acceso controlado a la clave de cifrado y debe ser auditado, tanto el acceso como la propia restauración.

c) Se deben mantener las prácticas recomendadas por el fabricante en cuanto a copias de seguridad.

d) Se recomienda realizar copias de seguridad periódicas. Al menos se debe generar una copia de seguridad incremental diaria que debe conservarse durante siete días. También debe generarse una copia de seguridad incremental semanal en domingo conservando la copia durante cuatro semanas. Además, debe generarse una copia incremental cada día uno de mes conservándose los doce últimos meses. Por último, debe generarse una copia de seguridad anual conservándose durante cinco años.

e) Almacenar las copias de seguridad en lugares distintos a la ubicación física del servidor de producción.

f) Se recomienda almacenar las copias de seguridad en sistemas de discos redundantes.

g) Realizar pruebas de recuperación periódicamente en forma de simulacro.

4.4.5 CIFRADO

El cifrado es la conversión de datos disponibles en un formato legible a otro formato codificado creando la necesidad de descifrarlos para procesarlos. El cifrado implica utilizar una clave criptográfica que se genera mediante unos valores matemáticos que acuerdan tanto el emisor como el receptor para convertir el contenido de un mensaje en un formato ilegible, permitiendo proteger la información de agentes externos y no autorizados.

Es responsabilidad de la organización conocer y asegurar los datos más sensibles que posee. Este hecho depende del contenido de la información de las distintas bases de datos. No todos los datos poseen la misma criticidad y corresponde a la organización categorizar primero la información, y posteriormente asegurar el acceso a ella en función de la sensibilidad del dato.

Se dispone de diversos protocolos de cifrado dependiendo del estado de la información en el que se encuentre. Así pues, se puede categorizar el cifrado de la siguiente manera:

h) **Cifrado en tránsito:** se consideran que los datos están en tránsito cuando se mueven entre dispositivos. Durante la transferencia de la información, los datos se encuentran en mayor riesgo debido a la necesidad de descifrar antes de transferir.

   Se conoce como cifrado integral al cifrado de datos durante la transferencia. El cifrado integral garantiza la protección de la privacidad de los datos, aunque éstos sean interceptados. Se recomienda usar protocolos de cifrado para el tráfico SQL entre clientes y servidores como AES, FIPS, Triple DES, TLS, etc.

i) **Cifrado en reposo:** se consideran datos en reposo cuando se recopilan y almacenan en discos duros, cintas de respaldo o en la nube, se considera que los mismos se encuentran inactivos y estables. Los datos en reposo siempre deben estar encriptados y para ello, puede usarse protocolos como AES, Triple DES, SHA, etc.

   Se recomienda, además, el cifrado de toda la base de datos, objetos que contiene, tablas, columnas, celdas, registros de auditoría y todas las copias de seguridad que se realicen, independientemente del medio donde se almacenen.

El Centro Criptológico Nacional dispone de guías de configuración específicas que recogen el detalle de Cifrado para las Bases de Datos entre otra información de relevancia para bases de datos de tipo Oracle y DB2.

a) RECOMENDACIONES DE SEGURIDAD PARA ORACLE DATABASE 19C.

b) RECOMENDACIONES DE SEGURIDAD PARA BASES DE DATOS DB2.

4.5 REVISIÓN DE SOFTWARE

Después de la instalación del producto y sus actualizaciones debe revisarse el estado de la solución. Los permisos de objetos ya asegurados pueden haber cambiado y deben ser revisados de nuevo.

Es importante revisar la documentación de los objetos afectados y revisarlos posteriormente. A nivel de software se deben realizar las siguientes tareas de mantenimiento de forma periódica:

a) Mantener la versión del motor actualizada.

b) Mantener las versiones de cualquier software dependiente al motor actualizada.

c) Se recomienda configurar alarmas de consumo y uso del motor de BD.

d) Se recomienda documentar todos los cambios en el motor de BD y tareas de administración.

e) Verificar que las cuentas de usuario no sean root en el sistema operativo.

f) Revisar las vulnerabilidades de cada componente perteneciente a la instalación. Se pueden consultar las vulnerabilidades conocidas (CVEs) por componente (CPE) en portales como el NIST.

g) En caso de que se publiquen vulnerabilidades y no hayan sido corregidas por el fabricante se debe reportar a los responsables superiores de seguridad.

h) Limpiar los ficheros temporales después de la instalación del producto, actualización o corrección de vulnerabilidades.

5. GLOSARIO

TLS: Transport Layer Security es un protocolo de comunicaciones cuyo principal objetivo es proporcionar privacidad e integridad de datos entre dos aplicaciones que se comunican. El protocolo está compuesto por dos capas: el protocolo de registro TLS y el protocolo de negociación (handshake) TLS. Durante la negociación TLS, se utiliza un algoritmo de clave pública para intercambiar de forma segura firmas digitales y claves de cifrado entre un cliente y un servidor. La información de identidad y la clave se utilizan para establecer una conexión segura para la sesión entre el cliente y el servidor. Una vez establecida la sesión segura, la transmisión de datos entre el cliente y el servidor se cifra mediante un algoritmo simétrico, como AES.

RCAC: Row and Column Access Control. Permite controlar el acceso a una tabla a nivel de fila, de columna o en ambos y se puede utilizar para complementar el modelo de privilegios de tabla, garantizando que la información esté protegida adecuadamente y que los usuarios solo tienen acceso al subconjunto de datos que se requieren para realizar sus tareas laborales y cumplir con normativas y regulaciones específicas.

LBAC: Label Based Access Control. Es un modelo de seguridad que está destinado principalmente a aplicaciones gubernamentales o con grados de clasificación conocidos, ya que requiere que los datos y los usuarios se clasifiquen con un conjunto fijo de reglas que se implementan.

DBA: Database Administrator.

FIPS: Federal Information Processing Standards. La Publicación 140-2 del Estándar federal de procesamiento de información (FIPS) es un estándar gubernamental de Estados Unidos que define los requisitos mínimos de seguridad para módulos criptográficos en productos de tecnología de la información, tal como se define en la sección 5131 de la Ley de reforma de la administración de tecnologías de la información de 1996.

LDAP: El protocolo ligero de acceso a directorios hace referencia a un protocolo a nivel de aplicación, que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.

SSL: Capa de sockets seguros, la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

Kerberos: Es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

OTP: Contraseña de un solo uso que sirve para una autenticación.

Social Sign-In Authentication: El inicio de sesión social es un inicio de sesión único para usuarios finales. Con la información de inicio de sesión existente de un proveedor de redes sociales como Facebook, Twitter o Google, el usuario puede iniciar sesión en un sitio web de terceros en lugar de crear una nueva cuenta específicamente para ese sitio web.

AES: Advanced Encryption Standard (AES), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos, creado en Bélgica. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

DES: Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

Triple DES: En criptografía, Triple DES se le llama al algoritmo que hace triple cifrado del DES.

SHA: Los algoritmos de hash seguro1 son una familia de funciones de hash criptográficas publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) como un estándar federal de procesamiento de información (FIPS) de EE. UU.

SIEM: Security Information and Event Management (SIEM) es un término de ciberseguridad donde los servicios y productos de software combinan dos sistemas: Security Information Management (SIM) y Security Event Management (SEM).

DDoS: En seguridad informática, un ataque de denegación de servicio, llamado también ataque DoS (por sus siglas en inglés, Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

CVE: Las Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, siglas CVE), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación. Además, suele también mostrarse un enlace directo a la información de la base de datos de vulnerabilidades del NIST (NVD), en la que pueden conseguirse más detalles de la vulnerabilidad y su valoración.

NIST: El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), llamada entre 1901 y 1988 Oficina Nacional de Normas (NBS por sus siglas del inglés National Bureau of Standards), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica.

RLS: Row-Level Security. La seguridad de nivel de fila le permite utilizar la pertenencia a un grupo o el contexto de ejecución para controlar el acceso a las filas de una tabla de base de datos.

6. TABLA RESUMEN DE MEDIDAS DE REFUERZO DE LA SEGURIDAD

ÁMBITO	NUM.	MEDIDA	MOTIVO
IMPLEMENTACIÓN SEGURA	1.	En sistemas Unix o Linux, se recomienda especificar diferentes nombres de usuario a los creados de forma predeterminada, independientemente del gestor de base de datos a implementar.	Evitar el uso de nombres predeterminados para planificar ataques a la base de datos.
	2.	En sistemas Windows, se recomienda cambiar esta configuración predeterminada y especificar unos nombres de usuarios distintos para cada función.	Evitar el uso de nombres predeterminados para planificar ataques a la base de datos.
	3.	Se recomienda crear identificadores de usuarios propietarios de instancias específicos para cada instancia, añadiéndolo solo como miembro del grupo propietario de la instancia y no usarlo en ningún otro grupo.	Disponer de un mayor control en el número de usuarios y grupos que pueden modificar la instancia.
	4.	Durante la instalación, se recomienda hacer uso de contraseñas robustas que cumplan las directivas de seguridad de la organización.	Minimizar la posibilidad de ataques por fuerza bruta.

ÁMBITO	NUM.	MEDIDA	MOTIVO
CONTROL DE ACCESO	5.	Se recomienda el uso de contraseñas seguras y robustas que contengan al menos 12 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.	Minimizar la posibilidad de ataques por fuerza bruta.
	6.	Se recomienda configurar tiempo máximo de vida de una contraseña no superior a los 180 días.	El tiempo limita al atacante para poner en peligro la contraseña de un usuario.
	7.	Se recomienda configurar políticas de bloqueo de cuentas.	Limitar los intentos de un atacante para acceder a los recursos del sistema.
	8.	Se recomienda configurar cuentas de usuario específicas para los servidores de aplicaciones.	Limitar la superficie de ataque.
	9.	Es recomendable establecer un doble factor de autentificación	Aumentar la seguridad en la identidad digital de los usuarios.
	10.	Se recomienda hacer uso de mecanismos robustos de autenticación y comunicación como SERVER, LDAP TLS o Kerberos.	Mejorar la seguridad y confiabilidad de los mecanismos de autenticación.
	11.	Se recomienda seguir el principio de mínimo nivel de privilegios, donde solo se permita a los usuarios acceder a la información y hacer las acciones que realmente necesitan.	Minimizar la superficie de exposición.
	12.	Se recomienda revisar y, si es necesario, revocar aquellos permisos de usuarios o grupos que no los necesitan.	Minimizar la superficie de exposición.
	13.	En escenarios donde se almacenen datos sensibles, se recomienda, además, revisar los privilegios, establecer controles de acceso granulares.	Evitar el acceso a los roles sensibles desde entornos poco confiables.
	14.	Se recomienda revocar los privilegios de acceso a los datos del DBA si realmente no tiene la necesidad de acceder a dichos datos.	De forma predeterminada, un DBA tiene acceso a cualquier tabla en su instancia de base de datos. Esto supone un riesgo, sobre todo si la cuenta se ha vulnerado o se producen abusos en el uso de estos privilegios.
	15.	Se recomienda comprobar que no se ha otorgado acceso de tipo público a ninguna base de datos.	Minimizar la superficie de exposición.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	16.	Se recomienda asignar privilegios a través de un modelo de roles, evitando la asignación directa a usuarios.	Mejorar el control y mantenimiento de los privilegios de acceso.
	17.	Se recomienda usar los controles de acceso del sistema operativo.	Evitar que los administradores del sistema operativo obtengan demasiado acceso.
	18.	Se recomienda asignar permisos de tipo DBA solo a través de un rol, y controlar el acceso a este rol mediante contextos de confianza.	Permite restringir el acceso únicamente a conexiones originadas desde equipos de confianza.
	19.	Se recomienda revocar el privilegio de crear bases de datos a todos los usuarios, excepto el DBA.	Minimizar la superficie de exposición.
AUDITORÍA	20.	Se recomienda revisar las necesidades de registro de eventos de auditoría y seleccionar únicamente aquellos eventos importantes para la organización o los que estén relacionados con la seguridad del sistema.	Controlar la información de auditoría generada, evitando datos no relevantes y problemas de almacenamiento que pueden derivar en pérdida de evidencias relevantes.
	21.	Se recomienda crear un rol AUDITOR y otorgar los privilegios necesarios para leer y administrar los eventos de auditoría.	Controlar quién y cómo se puede acceder a la información de auditoría.
	22.	Se recomienda controlar el acceso al rol AUDITOR mediante contextos de confianza.	Permite restringir el acceso únicamente a conexiones originadas desde equipos de confianza.
	23.	Se recomienda evitar que los ficheros de auditoría generados puedan ser copiados, modificados o eliminados directamente por el administrador del sistema operativo o por otro usuario no autorizado de la plataforma.	Evitar la exfiltración de datos o el acceso a información sensible de auditoría saltándose los mecanismos de seguridad de la base de datos.
	24.	Se recomienda hacer uso de un servicio centralizador (SIEM) de registros de auditorías.	Unificación de diversos orígenes de auditoría, facilitar la correlación de logs y evitar la pérdida o manipulación de evidencias.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	25.	Se recomienda cifrar los registros de autoría almacenados en el disco (datos en reposo), tanto en el servidor de bases de datos, como en el servicio centralizador de registros, en caso de disponer de uno.	Evitar la exfiltración de datos o el acceso a información sensible de auditoría saltándose los mecanismos de seguridad de la base de datos.
	26.	Se recomienda auditar todas las acciones del DBA.	Mantener un registro de auditoría de las acciones administrativas que puedan comprometer el sistema.
	27.	Se recomienda auditar el acceso de los usuarios, en particular aquellos que tengan acceso a los datos sensibles.	Mantener un registro de auditoría de las acciones de los usuarios.
	28.	Se recomienda auditar todos los accesos a las tablas importantes.	Mantener un registro de auditoría de las acciones que puedan comprometer el sistema.
	29.	Se recomienda auditar todos los intentos de crear bases de datos.	Mantener un registro de auditoría de las acciones administrativas que puedan comprometer el sistema.
	30.	Se recomienda auditar el acceso controlado a la clave de cifrado de las copias de seguridad.	Mantener un registro de auditoría de las acciones que pueden comprometer la información.
PROTECCIÓN DE COMUNICACIONES	31.	Se recomienda hacer uso del cifrado con los algoritmos seguros expuestos en la capa de comunicaciones, como TLS 1.2 o superior.	Evitar la captura de datos en tránsito a través de la red.
	32.	Se recomienda no cifrar los datos mediante el uso de algoritmos obsoletos.	Los siguientes algoritmos están obsoletos: DES, DES40, 3DES112, 3DES168, RC4_40, RC4_56, RC4_128 y RC4_256, por lo que no deben ser utilizados.
	33.	Se recomienda utilizar conjuntos de algoritmos de cifrado robustos avalados por el Centro Criptológico Nacional.	Evitar la explotación de vulnerabilidades en algoritmos débiles u obsoletos.
	34.	Implantación y configuración del firewall.	Aumentar el control del tráfico entrante y saliente de los puertos.
	35.	Se recomienda cambiar los puertos por defecto del fabricante.	Aumentar la seguridad de acceso.
	36.	Se recomienda revisar y configurar los puertos usados por todas las instancias del servidor.	Minimizar la superficie de exposición, habilitando únicamente los puertos de comunicaciones necesarios.

ÁMBITO	NUM.	MEDIDA	MOTIVO
PROTECCIÓN DE LA INFORMACIÓN	37.	Se recomienda diseñar y hacer uso de políticas de acceso granular a registros, columnas o filas en aquellos entornos donde existan regulaciones o normativas que cumplir y el acceso a los datos tenga que realizarse según el contexto de quien lo solicita.	Cumplir con el principio de "necesidad de conocer".
	38.	Se recomienda hacer uso del control de acceso basado en etiquetas a nivel de registros cuando se maneje información sensible o clasificada relacionada con entidades del gobierno.	Cumplir con el principio de "necesidad de conocer".
	39.	Se recomienda hacer uso del control de acceso basado en etiquetas a nivel de registros cuando las siguientes afirmaciones son ciertas: – Se conoce el grado de clasificación de los datos. – La clasificación de los datos se puede representar por una o varias etiquetas de seguridad. – Las reglas de autorización se pueden enlazar a los componentes de la etiqueta de seguridad.	Cumplir con el principio de "necesidad de conocer".
	40.	Se recomienda el control de acceso basado en etiquetas a nivel de columna cuando: – Se requiere proteger columnas sensibles de accesos no autorizados a los dueños de la tabla o incluso al DBA. – Se requiere proteger tablas completas de accesos no autorizados a los dueños de la tabla o incluso al DBA.	Cumplir con el principio de "necesidad de conocer".

ÁMBITO	NUM.	MEDIDA	MOTIVO
	41.	Se recomienda limitar la exposición de información confidencial ocultándolos a los usuarios sin privilegios mediante el enmascaramiento de datos dinámico. La disponibilidad de esta característica dependerá del fabricante.	Cumplir con el principio de "necesidad de conocer".
BACKUP	42.	Se recomienda cifrar todos los ficheros de backup e imágenes de archivo, independientemente del medio donde se almacenen.	Evitar el acceso no autorizado a las copias de seguridad.
	43.	Se recomienda garantizar que la restauración de cualquier copia de seguridad debe requerir un acceso controlado a la clave de cifrado y debe ser auditado, tanto el acceso como la propia restauración.	Evitar el acceso no autorizado a las copias de seguridad y registrar cualquier tipo de acceso mediante una auditoría.
	44.	Almacenar las copias de seguridad en lugares distintos a la ubicación física del servidor de producción.	Evitar la indisponibilidad de la información en caso de ataque o fallo del sistema.
CIFRADO	45.	Se recomienda el cifrado de toda la base de datos, objetos que contiene, tablas, columnas, celdas, registros de auditoría y todas las copias de seguridad que se realicen, independientemente del medio donde se almacenen.	Proteger la privacidad.
REVISIÓN DE SOFTWARE	46.	Se recomienda mantener la versión del motor actualizada y el software dependiente.	Corregir vulnerabilidades que puedan afectar a la base de datos.
	47.	Se recomienda la configuración de alarmas de consumo y uso del motor de base de datos.	Monitorizar los recursos del sistema previene de errores que pueden afectar el acceso a los datos.