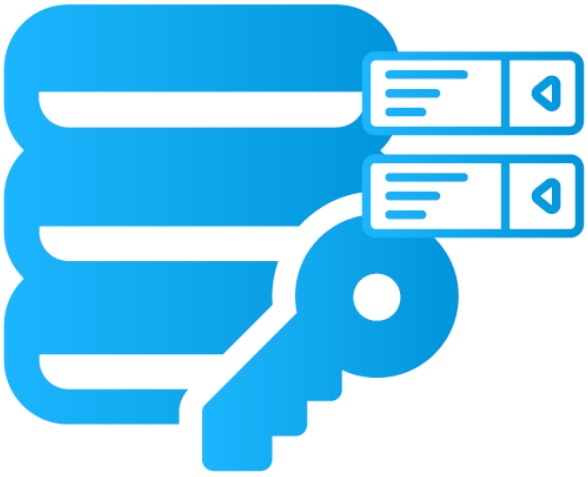
CCN
centro criptológico nacional

CCN-CERT BP/23

RECOMENDACIONES DE SEGURIDAD PARA BASES DE DATOS DB2



OCTUBRE 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
2021.10.22 11:14:36 +02'00'

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 de Seguridad 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.

octubre 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 con 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

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, por lo tanto, desde un punto de vista simplificado, se puede indicar que estará dividido en estos dos ámbitos de actuación:

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

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

El producto IBM DB2 es un gestor de bases de datos relacionales de tipo generalista, lo cual quiere decir que puede ser utilizado en múltiples entornos y aplicaciones, que se puede implementar tanto en sistemas Unix, Linux como servidores Microsoft Windows.

En todos los casos, será importante no perder de vista los aspectos de seguridad que se configuran en el ámbito del sistema operativo, como usuarios, servicios, comunicaciones y protocolos, así como los que se configuran en el entorno de DB2, como los procesos de autorización y control de acceso a los datos que residen en las distintas bases de datos.

La autenticación es el proceso por el cual un sistema verifica la identidad de un usuario. En DB2, este proceso se realiza fuera del entorno de la aplicación, a través de un módulo de autenticación. Mediante distintos módulos que incorpora DB2, se puede hacer uso de protocolos de autenticación como LDAP y Kerberos. Habitualmente la autenticación de los usuarios la realiza el sistema operativo o un servidor externo.

La autorización es el proceso de determinar si un usuario autenticado, dispone de acceso a la información y permisos que está solicitando. Este proceso se realiza íntegramente dentro de IBM DB2, consultando los permisos asociados a una identidad concreta. En este sentido, existen distintos tipos de permisos que pueden ser otorgados.

a) **Permisos primarios:** Aquellos que se otorgan directamente al identificador de autorización.

b) **Permisos secundarios:** Aquellos que se otorgan a grupos y roles de los cuales es miembro un identificador de autorización.

c) **Permisos públicos:** Aquellos que se otorgan a la entidad PUBLIC.

d) **Permisos basados en contexto:** Aquellos que se otorgan a un rol de contexto de confianza.

Estos permisos se pueden otorgar a los usuarios en varios niveles o categorías:

e) **Autorización a nivel de sistema:** Las autoridades administrador del sistema (SYSADM), el control del sistema (SYSCTRL), mantenimiento del sistema (SYSMAINT) y supervisor del sistema (SYSMON) proporcionan diversos grados de control sobre las funciones a nivel de instancia. Se trata de una forma de agrupar privilegios y controlar acciones como las operaciones de mantenimiento y otras tareas para instancias, bases de datos y objetos de base de datos.

f) **Autorización a nivel de base de datos:** Las autoridades administrador de seguridad (SECADM), administrador de la base de datos (DBADM), control de acceso (ACCESSCTRL), acceso a datos (DATAACCESS), administrador SQL (SQLADM), administrador de gestión de carga de trabajo (WLMADM), carga de datos en una tabla (LOAD) y conexión a una base de datos (CONNECT), proporcionan distintos grados de control dentro de la base de datos.

g) **Autorización a nivel de objeto:** La autorización a nivel de objeto implica la verificación de privilegios cuando se realiza una operación concreta sobre un objeto específico.

h) **Autorización basada en contenido:** Una forma de autorizar el acceso basado en contenido son las vistas. Las vistas permiten controlar qué columnas o filas de una tabla pueden ser leídas por usuarios específicos. Por otro lado, el control de acceso basado en etiquetas (LBAC) determina qué usuarios tienen permisos para leer y escribir filas y columnas individualmente.

Otro componente importante a la hora de definir la seguridad de un gestor de bases de datos es el cifrado, tanto de los datos en tránsito como de los datos en reposo. BD2 ofrece diferentes opciones de cifrado de los datos.

Para el cifrado de los datos en reposo, se dispone de las siguientes opciones:

a) Cifrado nativo de DB2 para cifrar bases de datos e imágenes de copia de seguridad.

b) La solución IBM InfoSphere Guardium Data Encryption para cifrar los datos del sistema

operativo subyacente y los archivos de copia de seguridad.

c) El sistema de archivos cifrados (EFS) de AIX para cifrar los datos del sistema operativo y los archivos de copia de seguridad.

Para cifrar los datos en tránsito entre clientes DB2 y bases de datos, se recomienda hacer uso del soporte nativo de TLS incluido en DB2 para comunicaciones entre:

a) Clientes y servidores DB2.

b) Nodos primarios y en espera en un entorno DB2 HADR

c) Clientes de DB2 y un servidor de federación de DB2.

Nota: El tipo de autenticación DATA_ENCRYPT está obsoleto y podría eliminarse en una versión futura. Para cifrar datos en tránsito entre clientes y bases de datos DB2, se recomienda utilizar el soporte del sistema de base de datos DB2 para TLS (Transport Layer Security). Además, DATA_ENCRYPT y SERVER_ENCRYPT utilizan algoritmos débiles que no son compatibles con las guías CCN-STIC, por lo que no deben ser utilizados.

3. IMPLEMENTACIÓN SEGURA DE LA BASE DE DATOS

Durante el proceso de instalación de la base de datos DB2 se crean un identificador de usuario (User ID), un grupo y una contraseña. Estos valores se crean por defecto si no son modificados durante la instalación. Dependiendo de la plataforma donde se realice la instalación de DB2, se crean distintos valores:

a) **Sistemas operativos UNIX y Linux:** El asistente de instalación crea, de forma predeterminada, el usuario “dasusr” para el DAS, “db2inst” para el propietario de la instancia y “db2fenc” como usuario delimitado (fenced user). Se recomienda especificar diferentes nombres de usuario a los creados de forma predeterminada.

   Si ya existe un usuario predeterminado, el asistente de instalación agrega un número del 1 al 99 al nombre predeterminado, hasta que se pueda crear un ID de usuario que aún no existe.

b) **Sistemas operativos Microsoft Windows:** el asistente de instalación crea, de forma predeterminada, un único nombre de usuario el usuario (db2admin) para el usuario DAS, el propietario de la instancia y los usuarios delimitados. Se recomienda cambiar esta configuración predeterminada y especificar unos nombres de usuarios distintos para cada función. A diferencia de los sistemas operativos Linux y UNIX, no se agrega ningún valor numérico al ID de usuario.

Tal y como se ha indicado anteriormente, DB2 puede utilizar los mecanismos de autenticación propios del sistema operativo para autenticar a los usuarios. Por ello, es muy recomendable especificar requisitos robustos de autenticación a nivel del sistema operativo.

En los sistemas operativos Linux y UNIX, las contraseñas no definidas se tratan como NULL y se considerará que cualquier usuario sin contraseña tiene una contraseña NULL. Desde la perspectiva del sistema operativo, esto es una coincidencia y el usuario será validado y podrá conectarse a la base de datos.

De forma predeterminada, el método de comunicación de ejecución de comandos en entornos de bases de datos particionadas en sistemas operativos Linux y UNIX, está basado en la herramienta “rsh”. Esta herramienta transmite las contraseñas en texto sin cifrar a través de

la red, lo que puede representar un riesgo de seguridad.

Se recomienda configurar la variable de registro DB2RSHCMD para establecer la ruta al ejecutable SSH para mejorar la seguridad en cualquier tipo de entorno.

```
# db2set DB2RSHCMD=/usr/bin/ssh -i
```

También es recomendable revisar y modificar los privilegios predeterminados que se han otorgado a los usuarios durante la instalación. De forma predeterminada, el proceso de instalación otorga privilegios de administración del sistema (SYSADM) a los siguientes usuarios en cada sistema operativo:

a) **En los sistemas operativos Linux y UNIX**, se le otorgan privilegios SYSADM a cualquier usuario válido que pertenezca al grupo primario del propietario de la instancia.

b) **En los sistemas Microsoft Windows**, se le otorgan privilegios SYSADM a los miembros del grupo de administradores locales y a la cuenta LocalSystem.

Si se ha configurado la enumeración de grupos (LOCAL o DOMAIN), entonces también se le aplicarán privilegios SYSADM al grupo de administradores en el controlador de dominio donde están definidos los usuarios. La variable de entorno DB2_GRP_LOOKUP permite controlar cómo DB2 realiza la enumeración de grupos en los sistemas Windows.

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.

De forma predeterminada, durante la instalación, la seguridad extendida se habilita en todos los productos DB2 instalados sobre Windows. En este caso, el instalador crea dos nuevos grupos DB2ADMNS y DB2USERS. A los miembros del grupo DB2ADMNS se le otorga también privilegios SYSADM.

A continuación, se muestran los privilegios asignados a cada grupo de usuarios cuando se utiliza la seguridad extendida de Windows.

PRIVILEGIO	DB2ADMNS	DB2USERS	MOTIVO
Create a token object (SeCreateTokenPrivilege)	Y	N	Manipulación de tokens (requerido para ciertas operaciones de manipulación de tokens y utilizado en autenticación y autorización)
Replace a process level token (SeAssignPrimaryTokenPrivilege)	Y	N	Crear proceso como otro usuario
Increase quotas (SeIncreaseQuotaPrivilege)	Y	N	Crear proceso como otro usuario
Act as part of the operating system (SeTcbPrivilege)	Y	N	Inicio de sesión de usuario
Generate security audits (SeSecurityPrivilege)	Y	N	Manipular registros de auditoría y seguridad

PRIVILEGIO	DB2ADMNS	DB2USERS	MOTIVO
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	Y	N	Modificar ACLs de objetos
Increase scheduling priority (SeIncreaseBasePriorityPrivilege)	Y	N	Modificar la memoria de trabajo de los procesos
Backup files and directories (SeBackupPrivilege)	Y	N	Manipulación del perfil y del registro (necesario para realizar determinadas rutinas de manipulación del registro y del perfil de usuario: LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex))
Restore files and directories (SeRestorePrivilege)	Y	N	Manipulación del perfil y del registro (necesario para realizar determinadas rutinas de manipulación del registro y del perfil de usuario: LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex))
Debug programs (SeDebugPrivilege)	Y	N	Manipulación de tokens (requerido para ciertas operaciones de manipulación de tokens y utilizado en autenticación y autorización)
Manage auditing and security log (SeAuditPrivilege)	Y	N	Generar entradas de auditoría
Log on as a service (SeServiceLogonRight)	Y	N	Ejecutar DB2 como servicio
Access this computer from the network (SeNetworkLogonRight)	Y	Y	Permitir credenciales de red (permite que el administrador de bases de datos DB2 use la opción LOGON32_LOGON_NETWORK para autenticarse, lo que tiene implicaciones de rendimiento)

PRIVILEGIO	DB2ADMNS	DB2USERS	MOTIVO
Impersonate a client after authentication (SeImpersonatePrivilege)	Y	N	Suplantación de cliente (necesario para que Windows permita el uso de determinadas API para hacerse pasar por clientes DB2: ImpersonateLoggedOnUser, ImpersonateSelf, RevertToSelf, etc.)
Lock pages in memory (SeLockMemoryPrivilege)	Y	N	Soporte de páginas grandes de memoria
Create global objects (SeCreateGlobalPrivilege)	Y	Y	Privilegio para crear objetos globales en una sesión de Terminal Services (requerido en Windows)

Por último, en todos los casos durante la instalación, se recomienda hacer uso de contraseñas robustas que cumplan las directivas de seguridad de la organización.

4. CONFIGURACIÓN SEGURA DE LA BASE DE DATOS

A continuación, se ofrecen una serie de recomendaciones para reforzar la seguridad de la base de datos DB2 una vez realizado el proceso de instalación.

4.1 CONTROL DE ACCESO

Diseñar unos controles de acceso adecuados y ajustados a las necesidades de explotación de los datos por parte de usuarios y herramientas es fundamental para reducir los riesgos de exfiltración o accesos no autorizados. La mayoría de las amenazas se engloban en esta categoría y se minimizan o directamente se eliminan manteniendo unos controles estrictos.

El acceso a una instancia o a una base de datos requiere que el usuario se autentique. DB2 proporciona distintos tipos de autenticación. El tipo de autenticación utilizado se almacena en el fichero de configuración en el servidor y se configura cuando se crea la instancia. Cada instancia puede tener su tipo de autenticación para acceder al servidor y a las bases de datos que se ejecutan en dicha instancia.

Se recomienda hacer uso de mecanismos robustos de autenticación como SERVER, LDAP o Kerberos y evitar hacer uso de autenticación CLIENT, sobre todo en aquellos entornos donde no se puede garantizar la seguridad del cliente.

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, minimizando la superficie de exposición.

Se recomienda revisar, y si es necesario, revocar aquellos permisos de usuarios o grupos que no los necesitan.

En escenarios donde se almacenen datos sensibles, se recomienda, además, revisar los privilegios, establecer controles de acceso granulares como Row and Column Access Control (RCAC) y Label Based Access Control (LBAC), a fin de evitar el acceso a los roles sensibles desde entornos poco confiables.

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. Se recomienda revocar los privilegios de acceso a los datos del DBA si realmente no tiene la necesidad de acceder a dichos datos.

Se recomienda comprobar que no se ha otorgado acceso PUBLIC a ninguna base de datos.

Un usuario no autorizado puede acceder a información que reside en tablas del sistema si no se han protegido adecuadamente. Se recomienda revisar y proteger las tablas importantes del sistema como Staging, Exception, SQL Replicated, Clone y Materialized Query Tables (MQTs)

Se recomienda asignar privilegios a través de un modelo de roles, evitando la asignación directa a usuarios.

Se recomienda usar los controles del sistema operativo para evitar que los administradores del sistema operativo obtengan demasiado acceso.

Se recomienda asignar permisos de tipo DBA solo a través de un rol, y controlar el acceso a este rol mediante contextos de confianza. Esto permite restringir el acceso únicamente a conexiones originadas desde equipos de confianza.

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

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.

El registro de las acciones no deseadas o accesos no autorizados a los datos y el análisis posterior mejora los niveles de control de acceso a los datos y la prevención de accesos no autorizados, accesos malintencionados o configuraciones inadecuadas.

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 en sus sistemas de base de datos.

La auditoría de DB2 genera y mantiene evidencias de auditoría para una serie de eventos de base de datos predefinidos. Los registros generados se guardan en un archivo de registro de auditoría y su análisis puede revelar patrones de uso que identificarían el mal uso del sistema. Una vez identificado, se pueden tomar acciones para reducir o eliminar dicho uso indebido del sistema.

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.

El administrador del sistema (que tiene la autorización SYSADM) puede utilizar la herramienta “db2audit” para configurar la auditoría a nivel de instancia, así como para

controlar cuándo se recopila dicha información de auditoría.

También se puede utilizar la herramienta "db2audit" para archivar los registros de auditoría de base de datos y de instancia, así como para extraer datos de auditoría de registros archivados de cualquier tipo.

El administrador de seguridad (que tiene autoridad SECADM dentro de una base de datos) puede usar políticas de auditoría, además de la función AUDIT de SQL para configurar y controlar los requisitos de auditoría para una base de datos individual.

El administrador de seguridad puede utilizar las siguientes rutinas de auditoría para realizar las tareas especificadas:

a) El procedimiento almacenado SYSPROC.AUDIT_ARCHIVE archiva los registros de auditoría.

b) La función de tabla SYSPROC.AUDIT_LIST_LOGS permite localizar registros de interés.

c) El procedimiento almacenado SYSPROC.AUDIT_DELIM_EXTRACT extrae datos en archivos delimitados para su análisis.

Desde el punto de vista de la información de auditoría generada, DB2 identifica los distintos eventos en diferentes categorías:

a) Auditoría (AUDIT). Genera registros cuando se cambia la configuración de auditoría o cuando se accede al registro de auditoría.

b) Comprobación de autorización (CHECKING). Genera registros durante la verificación de autorización de los intentos de acceder o manipular objetos o funciones de la base de datos DB2.

c) Mantenimiento de objetos (OBJMAINT). Genera registros al crear o liberar objetos de datos y al alterar ciertos objetos.

d) Mantenimiento de seguridad (SECMAINT). Genera registros cuando:

   i. Se otorgan o se revocan privilegios de objetos o autorizaciones de bases de datos.

   ii. Se otorgan o se revocan etiquetas de seguridad o excepciones.

   iii. Se altera la autorización de grupos, la autorización de roles o se anulan o se restringen atributos de una política de seguridad LBAC.

   iv. Se otorga o se revoca el privilegio SETSESSIONUSER.

   v. Se modifica cualquiera de los parámetros de configuración: SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP o SYSMON_GROUP.

e) Administración del sistema (SYSADMIN). Genera registros cuando se realizan operaciones que requieren autorización SYSADM, SYSMAINT o SYSCTRL.

f) Validación de usuario (VALIDATE). Genera registros al autenticar usuarios o recuperar información de seguridad del sistema.

g) Contexto de operación (CONTEXT). Genera registros para mostrar el contexto de la operación cuando se realiza una operación de base de datos. Esta categoría permite una mejor interpretación del archivo de registro de auditoría.

h) Ejecute (EXECUTE). Genera registros durante la ejecución de sentencias SQL.

Para cada categoría, se pueden generar directivas de auditoría que registren los fallos, los

aciertos o ambos. Habilitar todas las categorías y todos los eventos puede provocar un exceso de información y un elevado número de registros.

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.

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

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.

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.

Se recomienda hacer uso de un servicio centralizador de registros de auditorías.

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.

Se recomienda auditar todas las acciones del DBA.

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

Se recomienda auditar todos los accesos a las tablas importantes.

Si se requiere disponer de acceso directo a las tablas MQT (Materialized Query Tables), se recomienda habilitar la auditoría granular de todos los accesos SQL a dichas tablas.

Se recomienda auditar todos los intentos de crear bases de datos.

4.3 MEDIDAS DE PROTECCIÓN DE COMUNICACIONES

Db2 utiliza el protocolo TLS (Transport Layer Security) para transmitir datos de forma segura entre servidores y clientes.

Para proteger con el mayor grado de confiabilidad los datos en tránsito en todas las redes que utilizan TCP/IP se recomienda habilitar el uso de TLS 1.2 o superior y restringir el uso de SSL, TLS 1.0 o TLS 1.1.

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

Durante la negociación del protocolo TLS, el cliente y el servidor negocian qué conjunto de cifrado utilizar para intercambiar datos. Un conjunto de cifrado es un conjunto de algoritmos que se utilizan para proporcionar autenticación, cifrado e integridad de los datos.

Db2 utiliza GSKit que se ejecuta en modalidad FIPS para proporcionar soporte TLS. GSKit admite los siguientes conjuntos de cifrado:

CONJUNTOS DE ALGORITMOS SOPORTADOS POR GSKIT	
TLS_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

CONJUNTOS DE ALGORITMOS SOPORTADOS POR GSKIT	
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Durante la negociación DB2 selecciona automáticamente el conjunto de cifrado más fuerte admitido tanto por el cliente como por el servidor.

Si se requiere que el servidor acepte solo uno o más conjuntos de cifrado específicos, se puede establecer el parámetro de configuración “ssl_cipherspecs”:

a) Cualquiera de los valores anteriormente indicados.

b) Una combinación de valores, separando cada valor por una coma, sin espacios.

c) Null. En este caso, se seleccionaría el algoritmo más fuerte disponible.

Se recomienda verificar que se dispone de una versión reciente de DB2 donde se han deshabilitado los algoritmos de cifrado basados en 3DES. En caso contrario, se recomienda eliminar los siguientes conjuntos de algoritmos de la lista de valores en “ssl_cipherspecs”:

a) TLS_RSA_WITH_3DES_EDE_CBC_SHA.

b) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA.

c) TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA.

Nota: Estos algoritmos están deshabilitados a partir de las siguientes versiones: Db2 V10.5 FP9, Db2 V11.1.2.2 y Db2 V11.5.0.0.

Para habilitar TLS 1.2 en DB2, se recomienda hacer uso de certificados emitidos por una entidad de certificación de confianza.

La base de datos DB2 utiliza el puerto 523 para el Servidor de administración de DB2 (DAS), que utilizan las herramientas de la base de datos de DB2. Se recomienda revisar y configurar los puertos utilizados por todas las instancias del servidor utilizando el archivo de servicios para asignar el nombre del servicio en el archivo de configuración del administrador de la base de datos del servidor a su número de puerto.

Además, para entornos de bases de datos particionadas y entornos Db2 pureScale, si se ha establecido la variable de registro DB2_FIREWALL_PORT_RANGE, se recomienda permitir únicamente las conexiones en el rango de puertos especificado entre los miembros de la misma

instancia de DB2.

Si no se ha establecido esta variable de registro, se deben permitir conexiones en todos los puertos sin privilegios entre miembros de la misma instancia de DB2. Los puertos sin privilegios tienen números de puerto superiores o iguales a 1024.

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 ROW AND COLUMN ACCESS CONTROL (RCAC)

A partir de la versión 10.1 de DB2, se incorpora el soporte para configurar el control de acceso a filas y columnas (RCAC), como una capa adicional de seguridad de datos. RCAC controla 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.

Con esta característica, se puede garantizar que la información esté protegida adecuadamente y que los usuarios solo tienen acceso al subconjunto de datos que requieren para realizar sus tareas laborales y cumplir con normativas y regulaciones específicas.

Ventajas de RCAC:

a) RCAC 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) Incluso las autoridades de nivel superior, como los usuarios con autoridad DATAACCESS, no están exentos de estas reglas.

d) Solo los usuarios con autoridad de administrador de seguridad (SECADM) pueden administrar los controles de acceso a filas y columnas dentro de una base de datos.

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

f) Las aplicaciones, las herramientas de consulta improvisadas y las herramientas de generación de informes están todas sujetas a las reglas de RCAC. La aplicación está centrada en los datos.

g) No se requieren cambios en la aplicación para aprovechar esta capa adicional de seguridad de datos.

El modelo de seguridad basado en RCAC se centra en quién accede 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 RCAC 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 LABEL-BASED ACCESS CONTROL (LBAC)

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.

LBAC aumenta en gran medida el control que tiene sobre quién puede acceder a los datos, permitiendo decidir exactamente quién tiene acceso de escritura y quién tiene acceso de lectura a filas y columnas individualmente.

Por el contrario, RCAC es un modelo de seguridad de uso general destinado principalmente a clientes comerciales. Cualquier organización puede usar RCAC para crear sus propias reglas de seguridad, lo que a su vez permite una mayor flexibilidad.

Una política de seguridad LBAC incluye esta 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 esa 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 LBAC a nivel de registros cuando se maneje información sensible o clasificada relacionada con entidades del gobierno.

Se recomienda LBAC 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 LBAC.

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

Se recomienda LBAC a nivel de columna cuando:

a) Se requiere 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.

Debe tener en cuenta lo siguiente antes de implementar un modelo de seguridad basado en LBAC:

a) LBAC nunca permitirá el acceso a datos que estén prohibidos por el control de acceso discrecional.

b) Las directivas LBAC solo limitan el acceso a datos protegidos. No tienen ningún efecto en los datos no protegidos.

c) Las directivas LBAC no se verifican cuando quita una tabla o una base de datos, incluso si la tabla o la base de datos contiene datos protegidos.

d) Las directivas LBAC no se verifican cuando realiza una copia de seguridad de los datos. Si un usuario puede ejecutar una copia de seguridad de una tabla, las filas de las que se realiza una copia de seguridad no están limitadas de ninguna manera por la protección LBAC de los datos. Además, los datos en los medios de respaldo no están protegidos por LBAC. Solo los datos de la base de datos están protegidos.

e) LBAC no se puede utilizar para proteger ninguno de los siguientes tipos de tablas:

   i. Una tabla de aprovisionamiento (staging).

   ii. Una tabla de la que depende una tabla de aprovisionamiento (staging).

   iii. Una tabla de tipos (typed table).

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.

4.5 POLÍTICAS DE BACKUP

En ocasiones una deficiente política de protección de las copias de seguridad permite el acceso no autorizado a datos que han dejado de estar protegidos por la seguridad del servidor.

Si los datos almacenados en copias de seguridad se dejan desprotegidos, pueden ser accedidos directamente desde el servicio de backup.

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

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.

5. GLOSARIO

Autenticación: es el proceso por el cual un sistema verifica la identidad de un usuario. En DB2, este proceso se realiza fuera del entorno de la aplicación, a través de un módulo de autenticación. Mediante distintos módulos que incorpora DB2, se puede hacer uso de protocolos de autenticación como LDAP y Kerberos. Habitualmente la autenticación de los usuarios la realiza el sistema operativo o un servidor externo.

Autorización: es el proceso de determinar si un usuario autenticado, dispone de acceso a la información y permisos que está solicitando. Este proceso se realiza íntegramente dentro de IBM DB2, consultando los permisos asociados a una identidad concreta.

Cifrado nativo de DB2: El cifrado nativo de Db2 proporciona capacidad de cifrado incorporada para proteger las imágenes de copia de seguridad de la base de datos y los archivos clave de la base de datos de accesos no autorizados mientras se encuentran en un medio de almacenamiento externo. El cifrado es un componente clave en la protección de datos fuera de línea.

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.

HADR: High Availability Disaster Recovery. DB2 en Red Hat OpenShift es compatible con la recuperación ante desastres de alta disponibilidad (HADR) para proteger la base de datos contra la pérdida de datos. HADR proporciona una solución de alta disponibilidad ante fallos parciales y completos del sitio mediante la replicación de los cambios desde una base de datos de origen, llamada base de datos primaria, a las bases de datos de destino, llamadas bases de datos en espera.

Servidor de federación de DB2: un sistema federado es un tipo especial de sistema de gestión de bases de datos distribuidas (DBMS) que consta de una instancia de base de datos que funciona como servidor federado, una base de datos que actúa como base de datos federada, una o más fuentes de datos y clientes (usuarios y aplicaciones) que acceden a la base de datos y fuentes de datos. Un sistema federado sirve como base sobre la que se pueden construir una o más soluciones de virtualización de datos. Dentro de un sistema federado, una sola declaración SQL puede acceder a los datos que se distribuyen entre varias fuentes de datos.

Fenced user: El usuario delimitado (fenced) es un tipo de usuario que se utiliza para ejecutar funciones definidas por el usuario (UDF) y procedimientos almacenados fuera del espacio de direcciones utilizado por la base de datos DB2. El usuario predeterminado es db2fenc1 y el grupo predeterminado es db2fadm1.

DAS: DB2 Administration Server. El Servidor de administración de DB2 (DAS) es un punto de control que se utiliza únicamente para ayudar con las tareas en las instancias de la base de datos de DB2. Se debe tener un DAS en ejecución si desea utilizar herramientas como el Centro de replicación o el Centro de desarrollo. DB2 Administration Server (DAS) ha quedado en desuso y es posible que se elimine en una versión futura. DAS no se admite en entornos Db2 pureScale.

RSH: protocolo para la ejecución remota de comandos de consola para la administración de una base de datos DB2. No se recomienda utilizar rsh debido a que hace uso de algoritmos débiles de cifrado.

SSH: Secure Shell (SSH) es un protocolo para el inicio de sesión remoto seguro y otros servicios de red segura a través de una red insegura. SSH se puede utilizar como base para una serie de servicios de red seguros ya que proporciona un cifrado robusto, autenticación del servidor y protección de la integridad. También proporciona compresión de datos.

Seguridad extendida: Opción de instalación que está habilitada por defecto cuando se instala DB2 en sistemas operativos Windows. Esta opción de instalación crea dos grupos de seguridad (DB2ADMNS y DB2USERS) a nivel de sistema operativo y les otorga privilegios controlados.

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.

MQT: Materialized Query Tables. Las tablas de consulta materializada (MQT) son tablas cuya definición se basa en el resultado de una consulta. Las tablas MTQ almacenan en caché los resultados de una consulta y cuando se vuelve a ejecutar la consulta, el motor de la base de datos puede devolver los datos de la tabla de consulta materializada para mejorar el rendimiento. Los datos constan de resultados precalculados de las tablas que se indican en la definición de la tabla de consulta materializada.

GSKit: Global Security Kit. DB2 utiliza las capacidades criptográficas Global Security Kit (GSKit) para cifrar tanto los datos en reposo (cifrado nativo) como los datos en tránsito. El GSKit se utiliza para implementar los protocolos SSL y TLS que permiten las comunicaciones DB2 protegidas a través de la red.

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.

DB2 pureScale: Conjunto de tecnologías de IBM que ayudan a reducir el riesgo y el coste asociado con el crecimiento de la solución de base de datos distribuida proporcionando capacidad extrema y transparencia de aplicaciones. El Db2 pureScale environment está diseñado para ofrecer una disponibilidad continua y combina varios componentes de software integrados en una solución de base de datos de alta disponibilidad. Estos componentes se instalan y configuran automáticamente al desplegar DB2 pureScale Feature.

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.	Evitar el uso de nombres predeterminados para planificar ataques a la base de datos.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	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 configurar la variable de registro DB2RSHCMD para establecer la ruta al ejecutable SSH para mejorar la seguridad en este tipo de entornos	De forma predeterminada, en sistemas operativos Linux y UNIX, DB2 utiliza la herramienta rsh. Esta herramienta transmite las contraseñas en texto sin cifrar a través de la red, lo que puede representar un riesgo de seguridad.
	4.	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.	Permite disponer de un mayor control en el número de usuarios y grupos que pueden modificar la instancia.
	5.	Durante la instalación, se recomienda hacer uso de contraseñas robustas que cumplan las directivas de seguridad de la organización.	Minimiza la posibilidad de ataques por fuerza bruta.
CONTROL DE ACCESO	6.	Se recomienda hacer uso de mecanismos robustos de autenticación como SERVER, LDAP o Kerberos y evitar hacer uso de autenticación CLIENT, sobre todo en aquellos entornos donde no se puede garantizar la seguridad del cliente.	Mejorar la seguridad y confiabilidad de los mecanismos de autenticación.
	7.	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.
	8.	Se recomienda revisar y, si es necesario, revocar aquellos permisos de usuarios o grupos que no los necesitan.	Minimizar la superficie de exposición.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	9.	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.
	10.	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.
	11.	Se recomienda comprobar que no se ha otorgado acceso PUBLIC a ninguna base de datos.	Minimizar la superficie de exposición.
CONTROL DE ACCESO	12.	Se recomienda revisar y proteger las tablas importantes del sistema como Staging, Exception, SQL Replicated, Clone y Materialized Query Tables (MQTs)	Un usuario no autorizado puede acceder a información que reside en tablas del sistema si no se han protegido adecuadamente.
	13.	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.
	14.	Se recomienda usar los controles de acceso del sistema operativo.	Evitar que los administradores del sistema operativo obtengan demasiado acceso.
	15.	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.
	16.	Se recomienda revocar el privilegio de crear bases de datos a todos los usuarios, excepto el DBA.	Minimizar la superficie de exposición.
AUDITORÍA	17.	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.
	18.	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.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	19.	Se recomienda controlar el acceso al rol AUDITOR mediante contextos de confianza.	Permite restringir el acceso únicamente a conexiones originadas desde equipos de confianza.
	20.	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.
	21.	Se recomienda hacer uso de un servicio centralizador de registros de auditorías.	Unificación de diversos orígenes de auditoría, facilitar la correlación de logs y evitar la pérdida o manipulación de evidencias.
	22.	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.
	23.	Se recomienda auditar todas las acciones del DBA.	Mantener un registro de auditoría de las acciones administrativas que puedan comprometer el sistema.
	24.	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.
	25.	Se recomienda auditar todos los accesos a las tablas importantes.	Mantener un registro de auditoría de las acciones que puedan comprometer el sistema.
	26.	Si se requiere disponer de acceso directo a las tablas MQT (Materialized Query Tables), se recomienda habilitar la auditoría granular de todos los accesos SQL a dichas tablas.	Mantener un registro de auditoría de las acciones que puedan comprometer el sistema.
	27.	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.

ÁMBITO	NUM.	MEDIDA	MOTIVO
PROTECCIÓN DE COMUNICACIONES	28.	Se recomienda hacer uso del soporte nativo de TLS incluido en DB2 para comunicaciones entre: – Clientes y servidores DB2. – Nodos primarios y en espera en un entorno DB2 HADR – Clientes de DB2 y un servidor de federación de DB2.	Evitar la captura de datos en tránsito a través de la red.
	29.	Para cifrar datos en tránsito entre clientes y bases de datos DB2, se recomienda utilizar el soporte del sistema de base de datos DB2 para TLS (Transport Layer Security).	El tipo de autenticación DATA_ENCRYPT está obsoleto y podría eliminarse en una versión futura. DATA_ENCRYPT y SERVER_ENCRYPT utilizan algoritmos débiles que no son compatibles con las guías CCN-STIC, por lo que no deben ser utilizados.
	30.	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.
	31.	Se recomienda verificar que se dispone de una versión reciente de DB2 donde se han deshabilitado los algoritmos de cifrado basados en 3DES.	Las versiones más antiguas, hacen uso de algoritmos de cifrado débiles o vulnerables que no deben ser utilizados.
	32.	Se recomienda eliminar los siguientes conjuntos de algoritmos de la lista de valores en "ssl_cipherspecs": – TLS_RSA_WITH_3DES_EDE_CBC_SHA. – TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA. – TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA.	Los conjuntos de algoritmos que hacen uso de 3DES o SHA1 se consideran débiles o vulnerables y no deben ser utilizados.
	33.	Para habilitar TLS 1.2 en DB2, se recomienda hacer uso de certificados emitidos por una entidad de certificación de confianza.	Permite validar correctamente la cadena de emisión del certificado y por lo tanto su confianza.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	34.	Se recomienda revisar y configurar los puertos utilizados por todas las instancias del servidor utilizando el archivo de servicios para asignar el nombre del servicio en el archivo de configuración del administrador de la base de datos del servidor a su número de puerto.	Minimizar la superficie de exposición, habilitando únicamente los puertos de comunicaciones necesarios.
	35.	Para entornos de bases de datos particionadas y entornos Db2 pureScale, si se ha establecido la variable de registro DB2_FIREWALL_PORT_RANGE, se recomienda permitir únicamente las conexiones en el rango de puertos especificado entre los miembros de la misma instancia de DB2.	Minimizar la superficie de exposición, habilitando únicamente los puertos de comunicaciones necesarios.
PROTECCIÓN DE LA INFORMACIÓN	36.	Se recomienda diseñar y hacer uso de políticas RCAC 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.	Cumplir con el principio de “necesidad de conocer”.
	37.	Se recomienda hacer uso de LBAC a nivel de registros cuando se maneje información sensible o clasificada relacionada con entidades del gobierno.	Cumplir con el principio de “necesidad de conocer”.
	38.	Se recomienda hacer uso de LBAC 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 LBAC. – Las reglas de autorización se pueden enlazar a los componentes de la etiqueta de seguridad.	Cumplir con el principio de “necesidad de conocer”.

ÁMBITO	NUM.	MEDIDA	MOTIVO
	39.	Se recomienda LBAC 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".
	40.	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.	Evitar el acceso no autorizado a la información sensible fuera del ámbito de protección de la base de datos.
BACKUP	41.	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.
	42.	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.