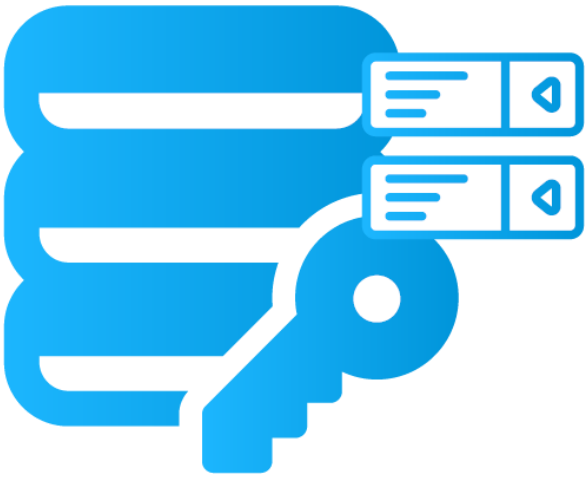
CCN
centro criptológico nacional

CCN-CERT BP/25

RECOMENDACIONES DE SEGURIDAD PARA BASES DE DATOS DB2 SOBRE zOS



FEBRERO 2022

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
2022.02.14 17:03:10 +01'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: febrero de 2022
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.

febrero de 2022

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. INTRODUCCIÓN

Las bases de datos se han convertido en el motor fundamental de las empresas, ya que, en ellas, se almacenan datos de carácter sensibles y todos aquellos datos que se necesitan para gestionar los organismos, desde nombres de clientes, a precios de un producto, o datos temporales almacenados para realizar modificaciones en aplicaciones críticas del entorno.

Dado que es un punto de acceso para todo tipo de ciberataques, se debe tener unas directrices claras a seguir para evitar la exposición a posibles vulnerabilidades.

La necesidad de este documento parte de ese punto en el que se deben imponer unas buenas prácticas y unas directrices en la implementación, modificación y mantenimiento de la base de datos.

El siguiente documento recoge las buenas prácticas y mejores praxis para el uso de IBM Db2 versión 12 de manera segura sobre sistemas Z.

A lo largo de los años, Db2 reconoce y aborda los siguientes problemas de seguridad:

a) Robo de privilegios o mala gestión

b) Manipulación de aplicaciones o servidores de aplicaciones

c) Manipulación de datos o registros

d) Robo de medios de almacenamiento

e) Acceso no autorizado a objetos.

Hay que tener en cuenta que las claves para esta tarea se basarán en los siguientes puntos clave:

f) Autenticación

g) Autorización

h) Integridad del dato

i) Confidencialidad

j) Integridad de los sistemas

k) Auditoría

Pero no solo se debe tener en cuenta el motor de nuestra base de datos, si no el entorno donde se despliega. Este punto será realmente importante para la seguridad y el manejo de las bases de datos.

En este documento, como ya se ha comentado, se centrará en el sistema operativo z/OS, con todo lo que puede conllevar el desplegar una base de datos en uno de los sistemas más securizables del mercado.

3. BUENAS PRÁCTICAS

Independientemente de la base de datos que se despliegue sobre el sistema operativo z/OS, siempre hay unas directrices de seguridad que se deben tener en cuenta.

El motor donde se despliega la base de datos proporciona los elementos fundamentales para las comunicaciones y los accesos a la base de datos, de ahí que la actualización y el mantenimiento del propio sistema operativo sea tan importante.

Una vez instalado el sistema operativo, se debe seguir los siguientes pasos recomendados para una buena práctica:

a) Actualización del sistema operativo donde se despliega la base de datos.

b) Aplicación de parches y actualizaciones recomendadas para solventar vulnerabilidades.

c) Suscripción a las noticias de seguridad sobre el sistema operativo z/OS y la base de datos Db2.

d) El uso de autorizaciones con autenticaciones por usuarios y contraseñas.

e) Criterios específicos de seguridad recomendados por los propios proveedores del sistema operativo.

4. REVISIÓN DE SOFTWARE

Una vez instalado el producto o tras el parcheado del mismo, se debe identificar que todo ha salido correctamente y que el nivel de seguridad sea el más alto posible, teniendo en cuenta las recomendaciones del fabricante para sus productos.

Es importante que cuando se realice cualquier tipo de actualización, se lea con detenimiento la documentación aportada para saber a qué afecta y qué se debe esperar.

A nivel de software se deben realizar las siguientes acciones:

a) Mantenimiento del producto en la última versión.

b) Mantenimiento del producto con la subida de FL intrínsecos de Db2. Y los APARs necesarios para el correcto funcionamiento de Db2 y sus utilidades.

c) Actualización de parches de seguridad y evolutivos del producto.

d) Verificar, cada cierto tiempo, las cuentas que tienen privilegios de usuario root, para ver si son las adecuadas y comprobar si se están reutilizando, clonando, o usando de manera improcedente.

e) Comprobar posibles vulnerabilidades tanto del software como del sistema operativo donde se ha desplegado.

f) Si se considera que se ha encontrado una vulnerabilidad, habrá que avisar al fabricante en la menor brevedad posible con una descripción detallada del problema y las situaciones donde se han visto las vulnerabilidades.

g) Si el fabricante sube un nuevo parche por una vulnerabilidad y las personas encargadas de actualizar los parches, no han realizado la actualización, hay que ponerse en contacto con el equipo de sistemas para que realicen el parcheo lo antes posible.

h) Limpiar ficheros temporales.

i) Mantener actualizado los sistemas que se hablen con la base de datos.

j) Mantener actualizado el motor donde corre la base de datos.

k) Mantener actualizados y comprobar que siguen siendo seguros los canales por los que se accede a la base de datos.

5. CONTROL DE ACCESO AL DATO

El acceso al dato puede darse por usuarios que quieran llamar a una información específica, como procesos del propio entorno. Es decir, desde terminales interactivas hasta Store Procedures locales o remotas, utilidades o transacciones CICS o IMS. También podrían venir desde aplicaciones que corren en batch, hasta aplicaciones que usan DDF o CLI o conexiones a través de JDBC.

Para que todo esto funcione correctamente, es recomendado utilizar diferentes usuarios y roles que puedan acceder a los datos con diferentes privilegios de seguridad, estos deberán darse según el acceso que necesite cada usuario o programa con un estudio previo de cada caso de uso.

Las autorizaciones se deben dar por cada vista, tabla, esquema, objeto, etc. Para ello habrá que:

a) Definir reglas de autorizaciones para los sistemas de Db2.

b) Definir niveles de seguridad dentro de los objetos de Db2.

c) Definir perfiles de usuario y roles que puedan acceder a los datos y la manera de acceder a ellos.

d) Se deben poder auditar las entradas a los datos para comprobar que se han creado unas reglas de seguridad acordes.

e) El sistema siempre debe ser capaz de conocer el origen de la petición o “quién” realiza la petición.

f) Se debe centralizar la creación, modificación y eliminación de las cuentas, identificadores, roles o grupos a un solo rol del administrador de la base de datos. Además, será el encargado de acreditar los diferentes niveles de seguridad según acordados con los roles de sistemas de seguridad.

5.1 PERMISOS POR ID DE USUARIO

Una de las maneras de escarizar las entradas de Db2, es a través del identificador principal o primario de usuarios, dándole privilegios desde Db2 a esos usuarios.

Se recomienda el uso de un identificador primario único por cada sistema/persona que desea acceder a los datos, y de un identificador secundario que se asociará al primario y al que se le asociará diferentes capas de seguridad. Es una de las maneras de poder identificar los permisos de accesos de cada usuario de manera masiva. Otorgar a una ID el privilegio de ejecutar un plan o paquete puede proporcionar un conjunto de privilegios finamente detallado y puede eliminar la necesidad de otorgar otros privilegios por separado.

5.2 PERMISOS POR ROLES

Además, se recomienda crear roles de usuario donde se puedan garantizar los privilegios a este nivel. Esta agrupación creada para categorizar a los usuarios o identificadores ayudará en la creación de perfiles de seguridad por agrupación de tipo de trabajos dentro de la base de datos.

Dentro de los roles que es posible encontrar, hay algunos básicos y comunes que se deberían tener en cuenta y crearlos en concordancia (estos no son los únicos roles que se pueden usar, pero si los mínimos recomendados).

a) **Rol de Administrador de seguridad:** Son los gestores de seguridad, además de las cuentas de los usuarios, las auditorías que deban hacerse o la gestión de las claves de cifrados.

b) **Rol de Administrador de Base de Datos:** Involucran una gran cantidad de tareas, desde la generación de base de datos, la actualización del software, comprobación del performance o el buen funcionamiento, el inicio y apagado de la base de datos e incluso de crear el respaldo que necesite la base de datos. Estos usuarios deberían tener privilegios de administración y modificación de las bases de datos.

   Es un rol que se debería dar solo a los administradores, y que una vez creada la base de datos se revoque el acceso a todo aquel que lo tenga menos a los administradores reales que se queden con el rol.

   Se deberá revisar este rol de manera periódica para comprobar que los identificadores asociados a este rol son los correctos.

c) **Rol de usuario de explotación de datos:** Este rol es adecuado para aquellos usuarios que son los encargados de hacer explotación y minería de datos de carácter de negocio. Estos usuarios suelen tener solo acceso de lectura.

d) **Rol de administrador de la aplicación:** Pueden ser cuentas que solo cuenten con los privilegios para la actualización y el parcheo de la aplicación.

e) **Rol de aplicación:** En esta categoría se podría englobar las cuentas de Identificadores que vengan por parte de aplicaciones externas o internas que necesiten ver los datos. En este

caso, suelen tener acceso de lectura y escritura en las tablas o datos necesarios para su aplicación.

f) **Rol de usuarios habituales de base de datos:** En este caso están englobados los identificadores con acceso restringidos a sus datos específicos, tablas, vistas y objetos.

5.3 ACCESO BASADO EN PROPIEDAD

La propiedad del objeto conlleva un conjunto de privilegios relacionados sobre el objeto. Db2 proporciona controles separados para la creación y propiedad de objetos.

Si desea evitar que los usuarios obtengan privilegios implícitos de la propiedad del objeto, puede convertir un rol de Db2 en el propietario del objeto. Para hacer esto, debe crear el objeto en un contexto confiable que se define con la cláusula ROLE AS OBJECT OWNER AND QUALIFIER.

5.4 ACCESO A MULTINIVEL

También conocido como el acceso multicapa, permite poder clasificar a los usuarios y roles con capas de seguridad. Estas capas se basan por una jerarquía de niveles de seguridad y no por categorías de seguridad.

Esta manera de acceder se ve beneficiada por el uso de la funcionalidad de seguridad multinivel del propio z/OS. Previniendo que usuarios no autorizados lleguen a clasificaciones donde no deben tener acceso.

Si se utiliza a nivel de fila, se puede definir unas políticas de seguridad muy fuertes para objetos de Db2 y realizar security checks a nivel de filas. Estos checks ayudan a visualizar que usuarios tienen autorización de ver, modificar o realizar cualquier otra acción sobre filas de datos.

Se recomienda el uso de este acceso multinivel en datos muy sensibles.

5.5 ACCESO EXTERNO

Puede controlar el acceso a Db2 utilizando una rutina de salida proporcionada por Db2 o una rutina de salida que usted escriba.

Si su instalación usa una de las rutinas de salida de autorización de control de acceso, puede usarla para controlar la verificación de autorización y autenticación, en lugar de usar otras técnicas y métodos.

5.6 ACCESO A NIVEL USUARIO

Cuando se crea un usuario que debe logarse con una contraseña, el administrador de la base de datos le enviará una contraseña provisional que deberá cambiar la primera vez que se conecte en el sistema. El cambio de contraseña debe venir con las siguientes pautas marcadas:

a) La contraseña no debe tener palabras como: USER, ADMINS, PUBLIC, GUESTS, cualquier palabra reservada de SQL.

b) Si se utiliza TSO, RACF, o alguna de las otras aplicaciones de seguridad que se pueden conectar, habrá que seguir las directrices marcadas por cada uno de esos aplicativos de

seguridad, ya que las contraseñas deberán seguir las pautas, como por ejemplo la longitud, de cada uno de esos sistemas.

c) Para que una contraseña sea fiable y segura es recomendable que:

i. Al menos tenga doce caracteres y como máximo quince.

ii. Que alterne entre mayúsculas y minúsculas.

iii. Que contenga al menos un número.

iv. Que contenga al menos un carácter especial (! # $ % & ' ( ) * + , - . / : ; < = > ? @ ^ _).

v. Que no contenga el nombre del usuario u otro nombre de cualquier rol.

vi. Que no contenga fechas de nacimiento, en general, fechas.

vii. Debe existir un número limitante de intentos de entrada con una contraseña errónea.

viii. Debe poder bloquearse un usuario después de un número de intentos fallidos (el límite de intentos no debería ser más de seis).

ix. Debe existir un límite de tiempo para sesiones externas que expiren y se pueda cerrar el sistema. (Lo recomendado son 90 minutos, pero hay que estudiar el caso de cada una de las aplicaciones o usuarios que realicen esta sesión)

x. Se debe renovar la contraseña al menos cada tres meses. Se recomienda crear recordatorios a nivel de usuario.

6. EL ACCESO AL SUBSISTEMA DE DB2

Se puede controlar los accesos a un subsistema Db2 externo con productos como RACF.

6.1 CONTROL DE ACCESO CON RACF

A continuación, se mostrará las ventajas que supone controlar la entrada a los subsistemas con RACF:

a) Identificar y verificar el identificador asociado al proceso que intenta entrar.

b) Conectar los identificadores a roles y grupos dados de alta en RACF. La base de datos de seguridad que se aplica sobre z/OS.

c) Auditar diferentes intentos de accesos a recursos protegidos.

Es recomendable utilizar el acceso a la base de datos a través del RACF siempre y cuando el sistema esté operativo en el mismo subsistema donde se encuentra la base de datos.

6.2 CONTROL DE ACCESO CON IMS TERMINAL SECURITY

IMS Terminal Security permite controlar y limitar las entradas de un código de transacción a un LTERM o grupos de LTERMS del sistema. Para proteger un programa en particular, se debe autorizar un código de transacción que se dará de alta en la lista de LTERMS. Alternativamente, puede asociar cada LTERM con una lista de los códigos de transacción que un usuario puede ingresar desde ese LTERM.

Este código será el que se pase a Db2 como identificador y esté dado de alta.

Se recomienda la utilización de este producto, siempre y cuando esté instalado en sistema operativo motor.

6.3 CONTROL DE ACCESO CON CICS TRANSACTION CODE SECURITY

CICS Transaction Code Security trabaja con RACF para controlar las transacciones y programas que pueden acceder a Db2, se puede activar o desactivar la opción en las operaciones de bind para limitar el acceso a subsistemas específicos de CICS.

Se recomienda el uso de este producto siempre que se utilicen transacciones CICS para llamadas a la base de datos y que esté implementado dentro del sistema.

6.4 LLAMADAS EN LOCAL Y EN REMOTO

6.4.1 LLAMADAS DESDE SISTEMAS LOCALES

Se podría utilizar el logon de TSO para logarse en sistemas internos.

Si se ejecuta Db2 con TSO y se está utilizando el logon de ID de TSO como ID primario de Db2, será el propio TSO el que verifica si el ID tiene acceso o no.

Se recomienda el uso de logon por TSO a todos los usuarios que tengan acceso a través de este sistema. Es recomendable, además, asignar como ID primario el usuario de TSO y seguir manteniendo un secundario para la aplicación de capas de seguridad.

Después de realizar estas acciones, el ID de autorización puede volver a utilizar los servicios de un sistema de seguridad externo.

Nota: Las contraseñas utilizadas por estos identificadores deben seguir los mismos consejos que un usuario de TSO.

6.4.2 LLAMADAS DE SISTEMAS REMOTOS

Es recomendable el uso de sistemas de seguridad que puedan gestionar, mantener y auditar este tipo de entradas.

Si sobre el motor hay desplegado un sistema de seguridad como RACF, se deberá usar este sistema para los accesos externos ya que, a través de sus funcionalidades, es capaz de validar varios checks de seguridad antes de poder entrar en el sistema.

Se recomienda las siguientes tareas para un motor desplegado sobre un sistema de seguridad RACF:

a) Verificar un ID asociado con una petición remota y chequear el ID mediante una contraseña.

b) Generar un “PassTicket” en el lado del que envía la petición. De esta manera se evita el envío de contraseñas a través de la red.

c) Verificar un ticket de Kerberos si su entorno distribuido usa Kerberos para administrar el acceso de los usuarios y realizar la autenticación de los usuarios.

d) Autenticar las entradas con Db2 Communication Database (CDB). Esto no es más que unas tablas en el catálogo de Db2 que se utilizan para establecer conversaciones con sistemas remotos.

7. AUDITORÍA

La auditoría de los accesos y permisos será un elemento clave a la hora de realizar una buena configuración de seguridad dentro de la implementación de Db2 12 sobre z/OS.

En ella se intentará supervisar cualquier entrada tanto de usuarios como de aplicaciones y diferenciarlos para que las personas encargadas de la revisión de esta auditoría sean capaces de distinguir entre amenazas o entradas comunes.

Gracias a la monitorización, se intenta responder a preguntas como, ¿Qué datos sensibles son los que requieren autorización?, ¿Quién tiene autorización para acceder a los datos?, ¿Quién ha accedido a los datos?, ¿Quién está intentando ganar privilegios para acceder a los datos?, ¿Qué intentos se hacen para obtener acceso no autorizado?

El catálogo de Db2 contiene información crítica de autenticación y autorización. Esta información proporciona la pista de auditoría principal para el subsistema Db2. Puede recuperar la información de las tablas del catálogo emitiendo consultas SQL.

La mayoría de las tablas de catálogo describen los objetos de Db2, como tablas, vistas, espacios de tabla, paquetes y planes. Otras tablas, particularmente aquellas con la cadena de caracteres "AUTH" en sus nombres, contienen registros de todos los privilegios y autorizaciones otorgados. Cada registro de catálogo de una subvención contiene la siguiente información:

a) Nombre del objeto

b) Tipo de privilegio

c) ID que reciben el privilegio

d) ID que otorgan el privilegio

e) Momento de la concesión

El seguimiento de auditoría de Db2 puede ayudarlo a monitorear y rastrear todos los accesos a sus datos protegidos. Los registros de rastreo de auditoría proporcionan otro rastro importante para el subsistema Db2. Puede utilizar el seguimiento de auditoría para registrar la siguiente información de acceso:

a) Cambios en los ID de autorización

b) Cambios en la estructura de los datos, como eliminar una tabla

c) Cambios en los valores de los datos, como actualizar o insertar registros

d) Intentos de acceso por identificaciones no autorizadas

e) Resultados de sentencias GRANT y sentencias REVOKE

f) Asignación de vales de seguridad de Kerberos a ID

g) Otras actividades de interés para los auditores

Se debe poder auditar a nivel de instancia como a nivel de base de datos, las recomendaciones que se deben seguir son las siguientes:

a) Activar el trace de Db2 para que pueda escribir en los logs.

b) Antes de activarlo, no grabará datos antiguos. Habrá que tener en cuenta la limpia de los logs cada cierto tiempo.

c) Elegir los elementos a auditar, se recomienda activar categorías de eventos como login, modificaciones, eliminaciones, etc. Según las necesidades, pero habrá que activar los eventos para poder ver toda la información en las trazas.

d) Audit trace usa el ID primario para hacer seguimiento de las modificaciones y entradas que se realicen, por lo que se recomienda que el ID primario sea entendible y visible para saber quién es la persona que entra (y utilizar el ID secundario para hacer una capa de seguridad según privilegios).

e) Generar reportes diarios y semanales sobre las trazas adquiridas en los que se pueda definir los siguientes elementos:

   i. Consumo de datos sensibles.

   ii. Privilegios mayores a diferentes IDs. (Se recomienda supervisar los ID con autoridades especiales y controlar cuidadosamente las identificaciones con privilegios sobre datos confidenciales Puede consultar el catálogo de Db2 para determinar qué ID tienen privilegios y autorizaciones en un momento determinado.)

   iii. Logins fallidos y número de intentos. (Si tiene datos confidenciales, use siempre la clase de auditoría de seguimiento 1).

f) Se recomienda crear un rol de auditor que sea la persona que tiene acceso a estos datos y pueda revisarlos.

g) Se recomienda que los reportes generados no sean modificables por el resto de los usuarios, ni siquiera por el auditor. Que, además, no puedan ser eliminados sin una operativa especial.

h) Se recomienda auditar todas las acciones de administrador de base de datos (encargado de dar privilegios o quitarlos al resto de roles).

i) Se recomienda auditar de manera específica los accesos a datos sensibles.

j) Se recomienda utilizar algún tipo de sistema que sea capaz de alertar si fuera necesario. Un sistema tipo SIEM que pueda generar alarmas de seguridad.

8. PROTECCIÓN DE LAS COMUNICACIONES

Para proteger con mayor grado los accesos a base de datos, se recomienda llevar acciones en los canales de comunicación con la base de datos.

a) Se recomienda hacer uso de los certificados emitidos por una entidad de certificación de confianza y hacer uso de los algoritmos de cifrados avalados por el Centro Criptológico Nacional.

b) Se recomienda hacer uso de herramientas de gestión de vulnerabilidades, donde se planifiquen análisis periódicos en busca de amenazas.

c) El despliegue de Db2 sobre z/OS soporta los protocolos TLS 1.0, SSL 3.0 y SSL 2.0.

9. CIFRADO

La recomendación contempla que se cifren los datos más sensibles de base de datos, para ello se pueden seguir las recomendaciones aportadas por el Centro Criptográfico Nacional (CCN) en sus documentos de referencia sobre Db2.

Db2 ya viene preparado para encriptar de manera transparente datos en reposo, como pueden ser los logs, catálogos, directorios, tablas e índices. La recomendación es utilizar las propias funcionalidades de Db2 para poder proteger esos datos en reposo.

Si se utiliza DFSMS, la recomendación es ampliar sus funciones para que puedan encriptar los datos dentro de Db2. De esta manera se puede optimizar la encriptación haciendo uso del hardware intrínseco del Z. (Disponible en zOS 2.2, RACF o ICIS u otro producto de seguridad).

Antes de poder utilizar el cifrado de conjuntos de datos DFSMS de z/OS para cifrar conjuntos de datos de Db2, asegúrese de que su sistema cumpla con los siguientes requisitos:

a) El sistema operativo es z/OS 2.2 o posterior. Para z/OS 2.2, se deben aplicar los PTF para APAR OA50569 y APAR OA53951.

b) El hardware necesario está instalado.

c) ICSF y RACF o productos de seguridad equivalentes.

d) El ID de usuario de la tarea iniciada de Db2 y cualquier ID de usuario que sea necesario para leer o escribir en un conjunto de datos cifrados tiene permiso para utilizar cualquier etiqueta de clave que se utilice para proteger los conjuntos de datos de Db2.

e) Cualquier etiqueta de clave que se utilice para proteger los conjuntos de datos de Db2 se define en todos los miembros de un grupo de intercambio de datos y en cualquier sistema de copia de seguridad que pueda leer o escribir desde un conjunto de datos cifrados.

f) Cualquier ID de usuario que se requiera para ejecutar cualquiera de las utilidades independientes está autorizado para usar cualquier etiqueta de clave que se use para proteger los conjuntos de datos de Db2.

g) Las actualizaciones de requisitos previos para que su producto de seguridad sea compatible con el cifrado de conjuntos de datos z/OS

Además, y al ser parte del sistema operativo z/OS, se puede securizar los datos con el uso de RACF ya comentado con anterioridad en este documento.

Si se quiere transportar datos de un sistema a otro, copiando, creando nuevas bases de datos, o compartiéndolo con otros sistemas habrá que tener en cuenta lo siguiente:

a) Si los datos son sensibles y existe la necesidad de compartirlos, se deberá crear un canal seguro que use un cifrado de datos en tránsito, y exista las autorizaciones necesarias para manejar de forma segura los datos en el destino.

b) Si son datos no sensibles, aun así, se recomienda crear un canal seguro para compartir los datos, y en la medida de los posible, que exista unas claves de cifrado para los datos en tránsito.

c) Para una situación de recuperación de desastres, si se debe acceder a los datos en otro sitio físico, entonces los perfiles ICSFkeys y RACF deben configurarse de manera similar al sitio

de origen. La misma regla se aplica a los sitios proxy y de origen de Db2 en el entorno de solución de disponibilidad continua de GDPS® con pérdida de datos cero

Adicionalmente se recomienda cifrar:

a) Los datos usados para la copia de seguridad.

b) Imágenes de archivo.

c) Datos protegidos por alguna de las leyes de protección de datos.

d) Logs que conlleven la modificación o regeneración de comandos.

10. POLÍTICAS DE BACKUP

Se exponen algunas buenas prácticas generales independientemente del producto o la versión:

a) Para la restauración de cualquier copia de seguridad se requiere un acceso controlado a la clave de cifrado y debe estar auditado, tanto el acceso como la restauración.

b) Se recomiendo la realización de copias de seguridad de manera periódica, al menos una incremental diaria y debe conservarse como mínimo siete días. Se recomienda la creación de una copia incremental de manera semanal que se conserve durante doce meses. Y una anual que se conserve durante cinco años.

c) Es recomendado que el almacenamiento de estas copias no esté en el mismo lugar físico donde se encuentra el sistema principal.

d) Es altamente recomendado, la realización de pruebas de restauración periódicas (al menos dos al año) para comprobar que el proceso de restauración funciona correctamente.

e) Es muy importante el mantenimiento y consistencia del dato, se recomienda utilizar la integridad referencial de Db2 para comprobar que la consistencia de los datos, tanto en los Backups, como los que están en tránsito, sean fiables y correctos.

10.1 COPIA DE SEGURIDAD, RECUPERACIÓN Y REINICIO

Aunque la alta disponibilidad de datos es un objetivo para todos los subsistemas de Db2, las interrupciones no planificadas son difíciles de evitar por completo. Sin embargo, una buena estrategia de respaldo, recuperación y reinicio puede reducir el tiempo transcurrido de una interrupción no planificada.

Para reducir la probabilidad y la duración de las interrupciones no planificadas, debe realizar copias de seguridad y reorganizar periódicamente sus datos para maximizar la disponibilidad de los datos para los usuarios y los programas.

Muchos factores afectan la disponibilidad de las bases de datos. Aquí hay algunos puntos clave a tener en cuenta:

a) Debe comprender las opciones de utilidades como COPY y REORG.

i. Puede recuperar en línea estructuras como espacios de tablas, particiones, conjuntos de datos, un rango de páginas, una sola página e índices.

ii. Puede recuperar espacios de tablas e índices al mismo tiempo para reducir el tiempo de recuperación.

iii. Con algunas opciones en la utilidad COPY, puede leer y actualizar un espacio de tabla mientras lo copia.

b) Los errores de E/S tienen los siguientes efectos:

i. Los errores de E/S en un rango de datos no afectan la disponibilidad para el resto de los datos.

ii. Si se produce un error de E/S cuando Db2 está escribiendo en el registro, Db2 sigue funcionando.

iii. –Si hay un error de E/S en el registro activo, Db2 pasa al siguiente conjunto de datos. Si el error está en el registro de archivado, Db2 asigna dinámicamente otro conjunto de datos.

c) Los métodos de recuperación ante desastres documentados son cruciales en el caso de desastres que puedan causar un apagado completo de su subsistema Db2 local.

d) Si se obliga a Db2 a un único modo de operaciones para el conjunto de datos de arranque o los registros, normalmente puede restaurar la operación dual mientras Db2 sigue ejecutándose. Db2 proporciona métodos extensos para recuperar datos después de errores, fallas o incluso desastres. Puede recuperar datos a su estado actual o a un estado anterior. Las unidades de datos que se pueden recuperar son espacios de tabla, índices, espacios de índice, particiones y conjuntos de datos. También puede utilizar las funciones de recuperación para realizar una copia de seguridad de un subsistema completo de Db2 o un grupo de intercambio de datos.

e) El desarrollo de procedimientos de copia de seguridad y recuperación es fundamental para evitar pérdidas de datos costosas y que consumen mucho tiempo. En general, asegúrese de que se implementen los siguientes procedimientos:

i. Crea un punto de consistencia.

ii. Restaure el sistema y los objetos de datos a un punto de consistencia.

iii. Realice una copia de seguridad y recupere el catálogo de Db2 y sus datos.

iv. Recuperarse de las condiciones fuera del espacio.

v. Recuperarse de una falla de hardware o energía.

vi. Recupérese de un error del componente z/OS.

Además, su sitio debe tener un procedimiento de recuperación en un sitio remoto en caso de desastre.

Los problemas específicos que requieren recuperación pueden ser desde un error de usuario inesperado hasta la falla de un subsistema completo. Puede ocurrir un problema con el hardware o el software; El daño puede ser físico o lógico. Aquí están algunos ejemplos:

a) Si ocurre una falla del sistema, un reinicio de Db2 restaura la integridad de los datos. Por ejemplo, un subsistema Db2 o un subsistema adjunto pueden fallar. En cualquier caso,

Db2 se reinicia automáticamente, revierte los cambios no confirmados y completa el procesamiento de los cambios confirmados.

b) Si se produce una falla en los medios (como un daño físico en un dispositivo de almacenamiento de datos), puede recuperar los datos hasta el punto actual.

c) Si los datos están dañados lógicamente, el objetivo es recuperar los datos a un punto en el tiempo antes de que ocurriera el daño lógico. Por ejemplo, si Db2 no puede escribir una página en el disco debido a un problema de conectividad, la página tiene un error lógico.

d) Si un programa de aplicación finaliza de manera anormal, puede usar utilidades, registros y copias de imágenes para recuperar datos a un punto anterior en el tiempo.

La recuperación de objetos Db2 requiere copias de imágenes adecuadas y conjuntos de datos de registro confiables. Puede utilizar una serie de utilidades y algunas estructuras del sistema para la copia de seguridad y la recuperación. Por ejemplo, la utilidad REPORT puede proporcionar parte de la información necesaria durante la recuperación. También puede obtener información del inventario de conjuntos de datos de registro del conjunto de datos de arranque (BSDS).

11. 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.

Db2: Representa el programa bajo licencia de Db2 o un subsistema de Db2 en particular. IBM renombró DB2 a Db2, y Db2 for z/OS es el nuevo nombre de la oferta anteriormente conocida como "DB2 for z/OS".

RACF: Representa las funciones proporcionadas por el componente RACF de z/OS Security Server.