****

Desarrollo – Estandarización SQL Server

Banco Solidario S.A. | Jefatura de Ingeniería y Producción

Manual de operaciones

2019

Tabla de contenido

[**1** **Objetivo** 1](#_Toc533606645)

[**2** **Antecedentes** 1](#_Toc533606646)

[**3** **Consideraciones** 1](#_Toc533606647)

[**4** **Arquitectura** 2](#_Toc533606648)

[4.1 Configuraciones Necesarias 2](#_Toc533606649)

[4.2 Diagrama de Tipo Entidad Relación 2](#_Toc533606650)

[4.3 Diccionario de Datos 3](#_Toc533606651)

[**5** **Seguridad** 4](#_Toc533606652)

[5.1 USO DE XP\_CMDSHELL 4](#_Toc533606653)

[5.2 USO DE CÓDIGO DSE (Dynamics String Execution) 4](#_Toc533606654)

[5.3 CADENAS DE CONEXIÓN CON USUARIOS SYSADMIN 5](#_Toc533606655)

[**6** **Transcripción de Código** 5](#_Toc533606656)

[**7** **Adopción de Prácticas** 7](#_Toc533606657)

[**8** **Consideraciones para Pases a Producción/Preproducción.** 7](#_Toc533606658)

1. **Objetivo**

Presentar al personal autorizado el documento que detalla los lineamientos de uso en Bases de Datos SQL Server para mantener una uniformidad en todo proceso de desarrollo que lleva a cabo el Banco y en vistas de mantener la Confidencialidad, Integridad y Seguridad de la información.

1. **Antecedentes**

REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – CIRCULAR ASFI/505/2017 DEL 4 DE DICIEMBRE DE 2017

SECCIÓN 6: GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE LA INFORMACIÓN (Art2. Administración de las bases de datos) La Entidad Supervisada debe realizar la administración de bases de datos, en función a procedimientos formalmente establecidos para este propósito, los cuales consideren mínimamente lo siguiente:

1. Instalación, administración, migración y mantenimiento de las bases de datos;
2. Definición de la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información;
3. Establecimiento de mecanismos de control de acceso a las bases de datos;
4. Documentación que respalde las actividades de administración de las bases de datos;
5. Realización de estudios de capacidad y desempeño de las bases de datos que permitan determinar las necesidades de expansión de capacidades y/o la afinación en forma oportuna.
6. **Consideraciones**

Los lineamientos de uso en SQL Server, principalmente apuntan a generar un ambiente de trabajo Seguro y más Eficiente, tanto para temas administrativos como para operaciones, desarrollo o troubleshooting. Para cumplir con estos objetivos se plantean tres aspectos importantes en la estandarización.

* Definición de Arquitectura.
* Seguridad en código TSQL.
* Transcripción TSQL

1. **Arquitectura**

Para la implementación de Base de Datos en ambientes productivos, se estandariza la selección de direcciones físicas donde residen los datos. Esta distribución está coordinada con el área de plataforma Central y debe ser considerada en cada diseño de Desarrollo de Software tanto interno como externo.

|  |  |
| --- | --- |
| DESCRIPCIÓN | RUTA FÍSICA |
| Archivos binarios de instalación de SQL Server | F:\ |
| Archivo de Datos de SQL Server | H:\DATA |
| Archivo de Logs de SQL Server | I:\LOG |
| Archivos de respaldos de Base de Datos | K:\RESPALDOS |

Todo diseño Software o aplicaciones que contengan conexiones a Base de Datos, deberán presentar documentación respecto a la Arquitectura definida representada principalmente en tres partes. Un detalle de requerimientos de configuración por parte del motor de Base de Datos, un diagrama de tipo Entidad Relación que mínimamente muestre las relaciones entre tablas, y un Diccionario de Datos con el detalle particular de objetos.

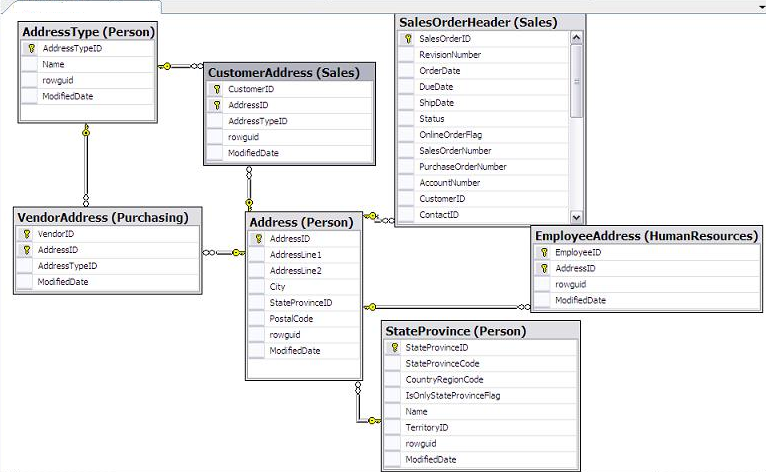
* 1. **Configuraciones Necesarias**

La información mínima que debe contener cualquier arquitectura en relación a la Base de Datos con la que se trabaja es la siguiente:

* Sistema Operativo Base (o contenedor). Ej. Windows Server 2019 Estándar, Docker
* Motor de Base de Datos. Ej. SQL Server 2017 Enterprise
* Idioma. Ej. Inglés, Español
* Server Collation. Ej. SQL\_Latin1\_General\_CP1\_CI\_AS
* Servicios requeridos. Ej. Reporting Services, Full Text Search

* 1. **Diagrama de Tipo Entidad Relación**

El diagrama de Tipo Entidad Relación, debe mostrar particularmente la relación que existiera entre las tablas de un Modelo Relacional en la arquitectura de Base de Datos. La herramienta con la cual se apoye para el diseño del diagrama no es limitativa, pero mínimamente debe poder observarse los nombres de los objetos principales. Como ejemplo puede observarse la imagen siguiente.



* 1. **Diccionario de Datos**

El Diccionario de Datos debe ser entregado en un formato de tabla Excel (ver Anexo 1), donde se registre la descripción de los campos utilizados por cada tabla parte de las Bases de Datos que son parte de la arquitectura propuesta en un sistema. Esta tabla debe contener mínimamente la siguiente información en el siguiente formato.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DB** | **TABLA** | **SCHEMA** | **COLUMNA** | **TIPO** | **MAXLENGTH** | **NULO** | **IDENTITY** | **DESCRIPCION** |
| AW | BusinessEntity | dbo | BusinessEntityID | int | 4 | NO | SI |  |
| AW | BusinessEntity | dbo | NationalIDNumber | nvarchar | 30 | NO | NO |  |
| AW | BusinessEntity | dbo | LoginID | nvarchar | 512 | NO | NO |  |
| AW | BusinessEntity | dbo | OrganizationLevel | smallint | 2 | SI | NO |  |
| AW | BusinessEntity | dbo | JobTitle | nvarchar | 100 | NO | NO |  |
| AW | BusinessEntity | dbo | BirthDate | date | 3 | NO | NO |  |
| AW | BusinessEntity | dbo | MaritalStatus | nchar | 2 | NO | NO |  |
| AW | BusinessEntity | dbo | Gender | nchar | 2 | NO | NO |  |
| AW | BusinessEntity | dbo | HireDate | date | 3 | NO | NO |  |
| AW | BusinessEntity | dbo | SalariedFlag | bit | 1 | NO | NO |  |
| AW | BusinessEntity | dbo | VacationHours | smallint | 2 | NO | NO |  |
| AW | BusinessEntity | dbo | SickLeaveHours | smallint | 2 | NO | NO |  |
| AW | BusinessEntity | dbo | CurrentFlag | bit | 1 | NO | NO |  |
| AW | BusinessEntity | dbo | rowguid | uniqueidentifier | 16 | NO | NO |  |
| AW | BusinessEntity | dbo | ModifiedDate | datetime | 8 | NO | NO |  |

Este detalle debe ser registrado por cada tabla de Base de Datos, con una descripción referencial de ella que será entregada en una hoja separada en el mismo documento Excel.

|  |  |  |
| --- | --- | --- |
| **DB** | **TABLA** | **DESCRIPCION** |
| AW | Address |  |
| AW | AddressType |  |
| AW | AWBuildVersion |  |
| AW | BillOfMaterials |  |
| AW | BusinessEntity |  |
| AW | BusinessEntityAddress |  |
| AW | BusinessEntityContact |  |

El archivo entregado deberá ser llamado: DiccionarioDeDatos.xlsx

1. **Seguridad**

Dentro de las definiciones de Seguridad en código TSQL para SQL Server, se definen tres principales puntos para consideración en el diseño de aplicaciones. Ninguno de este tipo de escenarios puede ser aplicado en código que será instalado en ninguno de los ambientes de Base de Datos del Banco.

Cuando se realice la adquisición de aplicaciones cerradas de terceros que contengan alguno de los escenarios señalados, deberá entregarse un documento al área de Seguridad de la Información explicando la necesidad irremplazable del uso de este tipo de codificación, para que el JNSI tenga presente en su Análisis de Riesgos las consideraciones necesarias.

* 1. **USO DE XP\_CMDSHELL**

La aplicación de XP\_CMDSHELL inicialmente requiere para su activación a un usuario de máximos privilegios en Base de Datos SQL Server, y para su uso requiere a un usuario con privilegios específicos que permitan las ejecuciones fuera de un entorno de Base de Datos.

* 1. **USO DE CÓDIGO DSE (Dynamics String Execution)**

El uso de programación dinámica, concatenación de cadenas para ejecución de código, uso de tablas para almacenamiento de fragmentos de código para construcción durante ejecuciones no está permitida en los entregables de aplicaciones que serán utilizados en el Banco.

* 1. **CADENAS DE CONEXIÓN CON USUARIOS SYSADMIN**

Todas las aplicaciones que tengan conexiones a Bases de Datos, deben ser entregadas con referencia a los permisos específicos que requiere sobre las bases que le correspondan. Es un requerimiento del área de Seguridad de la Información que la asignación de permisos sobre servidores de Base de Datos sea lo más específica y granular posible con el mayor grado de identificación posible. En este entendido, queda totalmente descartada la aceptación de aplicaciones que utilicen cadenas de conexión con usuarios de máximos privilegios de administración.

1. **Transcripción de Código**

En la escritura de código TSQL, es importante mantener una uniformidad en el código que permita una fácil lectura con la mayor claridad posible en el desarrollo de los flujos correspondientes. Para este propósito en general se debe considerar los siguientes aspectos referenciales en el código de ejemplo siguientes.

1. SEPARACIÓN DE INSTRUCCIONES

SELECT

(cnt.FirstName + ' ' + cnt.LastName) FullName,

emp.LoginID,

emp.Title

FROM HumanResources.Employee emp

INNER JOIN Person.Contact cnt

ON emp.ContactID = cnt.ContactID

ORDER BY cnt.LastName

* Separación de sentencias SELECT, FROM, WHERE, ORDER BY
* Separación de campos seleccionados de la vista
* Separación de sintaxis de JOINS a un nivel referencial a la tabla principal
* La separación se dará por tabulaciones como se muestra en el ejemplo

1. BLOQUES DE CÓDIGO

IF (@c = @d) OR (@c = 'ambos')

BEGIN

PRINT 'Condición correcta.'

END

ELSE

BEGIN

PRINT 'Condición incorrecta.'

END

* Separación de bloques identificables por la lógica del programa
* Preferentemente la separación se dará por tabulaciones como se muestra en el ejemplo

1. FORMATEO

* Uso de Mayúsculas en: SELECT, UPDATE, INSERT, DELETE, TRUNCATE, FROM, INNER JOIN, RIGHT JOIN, LEFT JOIN, CROSS JOIN, CROSS APPLY, WHERE, AND, OR, IN, LIKE, NOT, UNION, UNION ALL, EXCEPT, INTERSECT, BEGIN, END, IF, ELSE, SET, SUM, AVG, COUNT, MAX, MIN, GROUP BY, HAVING, ORDER BY, OVER, BETWEEN, PARTITION BY y funciones en general.
* Espacios entre valores/variables y operadores: =, <>, <, >, !=, ==, +, -, \*, /, ^
* Línea en blanco entre bloques o secciones de código
* Tabulación entre bloques internos
* Uso de alias en tablas para selección de columnas
* Cabecera comentada para Procedimientos Almacenados (ver Anexo 2)
* Comentarios referenciales/explicativos cortos en código
* No se comenta código desechado, código antiguo o ejemplos de ejecuciones

1. CONVENCIÓN EN NOMBRES

La referencia que se encuentra entre llaves <> debe ser cambiado por el nombre correspondiente según indicaciones siguientes.

Primary Keys:

* PK\_<NombreTabla>

Foreign Keys:

* FK\_<NombreTabla>\_<NombreTablaReferenciada>

Indexes:

* IX\_<NombreTabla>\_<Key1>\_<Key2>\_...<KeyN> (no considera includes)

General:

* No se usan tildes
* No se usan espacios
* No se usan palabras reservadas
* Procedimientos Almacenados no usan prefijo “sp\_”

1. ESTRUCTURAS

* No se utiliza tipos de datos TEXT, NTEXT, IMAGE
* No se utiliza tipos de datos NCHAR o NVARCHAR si no existe necesidad de caracteres Unicode
* Columnas de texto no utilizan default “NULL”
* No se utilizan procedimientos almacenados anidados

1. **Adopción de Prácticas**

En la codificación de TSQL para SQL Server, se deben considerar aspectos mínimos y básicos en sintaxis, metodología, diseño y mecanismos que permitan la aplicación de sistemas seguros, íntegros y de alta performance.

Para cumplir con este objetivo, se siguen las siguientes directrices:

1. No se usarán HINTS del tipo NOLOCK
2. No se usarán variables de tipo TABLE
3. No se altera el flujo con sintaxis GOTO
4. No se modifican objetos con sintaxis DROP, se utilizará sintaxis ALTER
5. No se usarán sentencias SELECT \*
6. No se usarán números de columnas en sentencias ORDER BY
7. Se debe usar alias de nombres de tablas para consultas que tienen 2 o más tablas referenciadas.
8. **Consideraciones para Pases a Producción/Preproducción.**

* Cualquier diseño de Software que involucre código SQL para Base de Datos y no cumpla principalmente con los lineamientos de seguridad establecidos, deberá registrarse en un documento entregado al JNSI para su validación y consideración en los Análisis de Riesgos que correspondan.
* Cuando se trate la verificación de software de terceros de código cerrado que no pueda ser modificado y no cumplan los lineamientos de Seguridad establecidos, se deberá mantener la documentación correspondiente y aclaratoria de los escenarios.
* Los scripts de creación de objetos (tablas, vistas, stored procedures, etc) serán entregados en archivos separados; uno por cada objeto. El nombre de cada archivo será igual al nombre del objeto referenciado y todos los archivos se encontrarán en una carpeta llamada “SCRIPTS”.
* La adopción de prácticas es obligatoria para la codificación de TSQL y su incumplimiento no dará curso a una implementación en ambientes del Banco.
* Los otros motores de Base de Datos deben aplicar todos los lineamientos del presente documento donde corresponda.