

Guía de Seguridad de las TIC CCN-STIC 884C

Guía de configuración segura para SQL Database





CCN-STIC 884C Guía de co

Guía de configuración segura para Azure SQL Database

Edita:



© Centro Criptológico Nacional, 2020

NIPO: 083-19-259-8

Fecha de Edición: enero de 2020

Plain Concepts ha participado en la realización y modificación del presente documento y sus anexos. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Guía de configuración segura para Azure SQL Database

<u>PRÓLOGO</u>

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán Secretario de Estado Director del Centro Criptológico Nacional



<u>ÍNDICE</u>

1. GUÍA DE CONFIGURACIÓN SEGURA PARA AZURE SQL DATABASE
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA5
2. DESPLIEGUE DE AZURE SQL DATABASE5
2.1 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL
2.2 DESPLIEGUE DE AZURE SQL DATABASE MEDIANTE POWERSHELL
2.2.1.1 DESPLIEGUE POWERSHELL
2.2.1.2 DESPLIEGUE POR EL PORTAL AZURE6
3. CONFIGURACIÓN DE AZURE SQL DATABASE9
3.1 MARCO OPERACIONAL
3.1.1 CONTROL DE ACCESO
3.1.1.1 IDENTIFICACIÓN9
3.1.1.2 REQUISITOS DE ACCESO
3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS12
3.1.1.4 MECANISMO DE AUTENTICACIÓN14
3.2 EXPLOTACIÓN
3.2.1 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS16
3.2.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS17
3.2.3 MONITORIZACIÓN DEL SISTEMA19
3.3 MEDIDAS DE PROTECCIÓN22
3.3.1 PROTECCIÓN DE LAS COMUNICACIONES22
3.3.1.1 PERÍMETRO SEGURO22
3.3.2 PROTECCIÓN DE LA INFORMACIÓN23
3.3.2.1 CALIFICACIÓN DE LA INFORMACIÓN23
3.3.2.2 COPIAS DE SEGURIDAD (BACKUP)24
3.4 SCRIPTS DE CONFIGURACIÓN
4. GLOSARIO Y ABREVIATURAS 27
5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD



CCN-STIC 884C Guía de configuración segura para Azure SQL Database

1. Guía de configuración segura para Azure SQL Database

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo del presente guía es seguir las recomendaciones de seguridad en la utilización del servicio Azure SQL Database cumpliendo con los requisitos necesarios del Esquema Nacional de Seguridad en su categoría ALTA.

Azure SQL Database es una base de datos relacional de propósito general como servicio (DBaaS) basada en la última versión estable de Microsoft SQL Server Database Engine, de alto rendimiento, fiable y segura que puede utilizar para crear aplicaciones y sitios web basados en datos en el lenguaje de programación de su elección, sin necesidad de gestionar la infraestructura.

2. DESPLIEGUE DE AZURE SQL DATABASE

2.1 Prerrequisitos para el despliegue mediante PowerShell

A continuación, se detallan los prerrequisitos para el despliegue de la instalación de SQL Database.

Requisitos de sistema:

Como requisito de sistema operativo es recomendable que consulte el siguiente link de Microsoft.

https://docs.microsoft.com/es-es/powershell/scripting/install/windows-powershell-system-requirements?view=powershell-6

Instalación PowerShell

- 1. Se debe conectar al módulo de PowerShell.
- 2. Instalar el módulo desde Powershell.

Install-Module -Name Az -AllowClobber -Scope CurrentUser

2.2 Despliegue de Azure SQL Database mediante PowerShell

El despliegue de Azure SQL se puede realizar desde el portal de Azure o bien desde el script que se comenta a continuación.

Nota: Es importante que en el script se escriba el nombre que tendrá el servidor y la ubicación donde se va a desplegar.

2.2.1.1 Despliegue Powershell

1. Copiar el contenido del script y ejecutar en PowerShell.



Guía de configuración segura para Azure SQL Database

Se declaran las variables que son necesarias para la ejecución del script. # # \$serverName= "Nombre del Servidor" # \$Location= "Nombre de localización Ej. "Nort Europe"" # \$resourceGroupName= "Nombre del Grupo de Recursos donde se creará el servidor" \$databaseName = "Nombre de la base de datos" # # \$adminSqlLogin = "Nombre Administrador de la base de datos" \$Password= "Escriba la contraseña" # # # ## Se encripta la contraseña de la variable Password para securizarla. \$PasswordSegura = ConvertTo-SecureString -String \$Password -AsPlainText -Force # ## Para la creación del servidor que albergara la base de datos se necesita crear el # objeto credencial donde contendrá el nombre del usuario administrador y la contraseña segura. # \$credentialObject = New-Object -TypeName System.Management.Automation.PSCredential ` -ArgumentList \$adminSqlLogin,` \$PasswordSegura # # ##Creamos el servidor en Azure con los parámetros definidos previamente \$server = New-AzSqlServer -ResourceGroupName -ServerName **\$serverName** # # -Location **\$location** -SqlAdministratorCredentials \$credentialObject ## Creamos la base de de datos en el servidor creado previamente # # \$database = New-AzSqlDatabase -ResourceGroupName \$resourceGroupName # -ServerName **\$serverName** # -DatabaseName \$databaseName -RequestedServiceObjectiveName "S0"

2.2.1.2 Despliegue por el portal Azure.

1. Buscar SQL Database.

Microsoft Azure					$ {\cal P} $ sql database	×
«	Servicios de J	Azure Vertodos	(más de 100) > Cr	ear un recurso	Servicios	– Los 13 resultados
Crear un recurso	_			_	👼 SQL Database	
🛧 Inicio				SQL	🐴 Almacenes de SQL Data Warehouse	
⊡ Panel	Máquinas	App Services	Cuentas de	SQL Database	🗣 Bases de datos de extensión de SQL Serve	
∃ Todos los servicios	virtuales		almacenamiento		🧧 Servidores de Azure Database for MySQL	

2. Pulsar en [agregar].



Guía de configuración segura para Azure SQL Database

Microsoft Azure		
	«	Inicio > SQL Database
+ Crear un recurso		SQL Database
🛧 Inicio		+ Agregar 🕓 Reservas 📑 Editar columnas 💍 Actualizar
🖽 Panel		
∃ Todos los servicios		Pruebe el nuevo explorador de recursos de SQL de Azure. Esta experie
+ FAVORITOS		
Todos los recursos		Suscripciones:
Srupos de recursos		Filtrar por nombre Todos lo
S App Services		1 elementos
Function App		NOMBRE TI ESTADO

3. Se debe seguir el asistente de configuración.

Microsoft Azure		𝒫 Buscar recursos, servicios y documentos (G-				
«	Inicio > SQL Database > Crear base de datos SQL					
+ Crear un recurso	Crear base de datos SQL					
📼 Panel	Básico Configuración adicional Etiquetas Revisar y crear					
∃ Todos los servicios	Cree una base de datos SQL con la configuración que prefiera. Complete la pestaña de configuración básica y, a					
★ FAVORITOS	continuación, vaya a Revisar y crear para efectuar el aprovisionamiento con valores predeterminados automáticos, o bien visite cada pestaña para personalizarlos. Más información 🖄					
Todos los recursos						
🕅 Grupos de recursos	Detalles del proyecto					
S App Services	Seleccione la suscripción para administrar recursos implementados y los costes carpetas para organizar y administrar todos los recursos.	s. Use los grupos de recursos como				
Function App						
👼 SQL Database	- Suscripcion	~				
Azure Cosmos DB	Grupo de recursos CCN-RG-SQL Crear nuevo	~				

4. Se debe crear un nuevo grupo de recursos.

Nota: *Para una gestión más avanzada hay que recurrir al apartado* [2.3 *Gestión de recursos Azure/Grupo de recursos*] *de la guía.* [CCN-STIC-884A - Guía de configuración segura para Azure].

Nombre de la base de datos: Definir un nombre para la base de datos.

5. Servidor: Pulsar en [crear nuevo].

detalles de la base de datos				
Indique la configuración necesaria para esta base de datos, incluida la selección de un servidor lógico y la configuración de los recursos de proceso y almacenamiento.				
* Nombre de la base de datos DATABASE-CCN				
* Servidor 🕜	Seleccionar un servidor Crear nuevo	~		

6. Se debe rellenar los campos que se solicita para el nuevo servidor.



Nuevo servidor	×
Microsoft	
* Nombre del servidor	
ccnbbdd	~
.database.wind	lows.net
* Inicio de sesión del administrador del servidor	
ccnadmin	~
* Contraseña	
	~
* Confirmar contraseña	
	~
* Ubicación	
(Europa) Norte de Europa	\sim
Permitir que los servicios de Azure accedan al ser	vidor

- Nombre del servidor: Nombre que tendrá la máquina virtual.
- Inicio de sesión del administrador del servidor: Usuario Admin local
- **Contraseña:** Se recomienda una contraseña compleja.
- Ubicación: Seleccionar Norte de Europa
- Permitir que los servicios de Azure accedan al servidor: La opción de Permitir que los servicios de Azure accedan al servidor debe estar desmarcada.
- Quiere usar un grupo elástico de SQL: Es recomendable seleccionar el grupo elástico que le permite administrar el rendimiento de múltiples bases de datos y almacenamiento compartido configurando límites.
- Grupo elástico: Pulsar en [crear nuevo]

* ¿Quiere usar un grupo elástico de SQL? ①	● Sí ◯ No			
* Grupo elástico 🚯	Seleccione un grupo elástico.	~		
	Crear nuevo			
7. Pulsar en [revisar y crear].				

t : Configuración adicional >

Nota: La implementación del recurso puede tardar varios minutos hasta su finalización. Una vez haya finalizado verá la siguiente información.



Guía de configuración segura para Azure SQL Database

Ø	Se completó la implementación				
8	Nombre de implementació Suscripción: Grupo de recursos: CCN-F	n: Microsoft.SQLDatabase. RG-SQL	newDatabase	Hora de inicio: 30/8/2019 9:34:59 Id. de correlación: e482cfb4-4442-4f79-ac7e-a7a4345ee;	781
^	Detalles de implementaci	ón (Descargar)			
	RECURSO	TIPO	ESTADO	DETALLES DE LA OPERACIÓN	
0	ccnbbdd/Default	Microsoft.Sql/servers/vu	Created	Detalles de la operación	
Ø	ccnbbdd/Default	Microsoft.Sql/servers/se	Created	Detalles de la operación	
Ø	ccnbbdd/DATABASE-CCN	Microsoft.Sql/servers/da	Created	Detalles de la operación	
Ø	ccnbbdd/AllowAllWindow	Microsoft.Sql/servers/fir	Created	Detalles de la operación	
ø	sqlvajjubm6xrdoheu	Microsoft.Storage/stora	OK	Detalles de la operación	
0	sqlvajjubm6xrdoheu	Microsoft.Storage/stora	ОК	Detalles de la operación	
0	ccnbbdd	Microsoft.Sql/servers	Created	Detalles de la operación	
0	sqlvajjubm6xrdoheu	Microsoft.Storage/stora	ОК	Detalles de la operación	

3. CONFIGURACIÓN DE AZURE SQL DATABASE

3.1 Marco operacional

3.1.1 Control de Acceso

3.1.1.1 Identificación

Azure AD proporciona la administración de identidades basada en la nube y permite usar una identidad única en todo su *Tenant* y las aplicaciones de acceso en Azure.

Se recomienda que para la gestión de los administradores se utilice Azure Active directory en la gestión de cuentas de administradores y delegación en base de datos.

Nota: *Para una gestión más avanzada hay que recurrir al apartado* [3.1.1 Azure Active Directory / Alta, baja y modificación de cuentas y grupos] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.2 Requisitos de acceso

En esta guía se trata la seguridad en el acceso a los servidores de SQL Database.

Para ello, se debe aplicar una capa de seguridad mediante RBAC creando un nuevo rol personalizado, permitiendo dar un privilegio de administración a los servidores de SQL.

Nota: Recordar que tan sólo los usuarios que tengan permisos de creación de roles pueden crearlos.

Los permisos son:

Microsoft.Authorization/roleDefinitions/write

Microsoft.Authorization/roleDefinitions/delete

Creación de ROL personalizado.

1. Desde Powershell ejecutar:



CCN-STIC 884C Guía de configuración segura para Azure SQL Database

New-AzRoleDefinition -InputFile "c:\temp\SQLAdmRole.json"

Nota: El fichero SQLAdmRole.Json se puede encontrar adjunto en el apartado de Scripts de Configuración de la presente guía.

Al ejecutar este comando devuelve esta información.

Administrador: Windows PowerShell						
PS C:\WINDOWS\sy:	<pre>S C:\WINDOWS\system32> New-AzRoleDefinition -InputFile "c:\temp\SQLAdmRole.json"</pre>					
Name	: SOLADMIN					
Id	: cla58e11-0521-455f-b505-516aab72d904					
IsCustom	: True					
Description	: Utilizado para gestionar SQL PaaS de Azure.					
Actions	: {Microsoft.Authorization/*/read, Microsoft.Insights/alertRules/*,					
	Microsoft.ResourceHealth/availabilityStatuses/read, Microsoft.Resources/deployments/*}					
NotActions	: {Microsoft.Sql/managedInstances/databases/currentSensitivityLabels/*,					
	Microsoft.Sql/managedInstances/databases/recommendedSensitivityLabels/*,					
	Microsoft.Sql/managedInstances/databases/schemas/tables/columns/sensitivityLabels/*,					
	Microsoft.Sql/managedInstances/databases/securityAlertPolicies/*}					
DataActions	: ()					
NotDataActions	: ()					
AssignableScopes	: {/subscriptions/965c7398-06c7-4edf-87ee-35744843942b}					

Nota: Recordar que puede comprobar este nuevo ROL desde el portal tal y como se indica a continuación.

- 1. Pulsar en todos los recursos.
- 2. Buscar el nuevo servidor de SQL.
- 3. Pulsar en [Control de acceso/Roles].

Microsoft Azure				rsos, servicios y documentos	(G+/)	
	« Inicio > Todos los recursos >	ccnbbdd - Control d	le acceso (IAM)			
+ Crear un recurso	Todos los recursos	« ×	ccnbbdd - Control de ac	ceso (IAM)		
 Inicio Panel 	+ Agregar	••• Más	, Buscar (Ctrl+/)	🕂 Agregar 🛛 🗮 Edit	tar columnas 💍 Actu	alizar 💼 R
∃ Todos los servicios	CCNBBDD		🗟 Información general	Comprobar acceso	Asignaciones de roles	s Asignaciones d
- 🛨 FAVORITOS			Registro de actividad	Una definición de roles e	es un conjunto de permi	sos. Puede usar los re
I Todos los recursos	👼 ccnbbdd		🝰 Control de acceso (IAM)	propios personalizados.	Más información 🛛	
(😭 Grupos de recursos				Nombre 👩	Tipo 🚯	
(App Services			🗙 Diagnosticar y solucionar pr	SQLADMIN	Todo	
🦘 Function App			Configuración	Se muestran 1 de 17 ro	les.	
🗟 SQL Database			📣 Inicio rápido	NOMBRE		
🖉 Azure Cosmos DB			🌻 Grupos de conmutación por	🔓 SQLADMI	IN @	
C			<u></u>			

Desde ahí se puede ver el rol.

Asignación del nuevo rol

- 1. Pulsar en [todos los recursos].
- 2. Seleccionar la base de datos.
- 3. Pulsar en [Control de acceso/Agregar]



Guía de configuración segura para Azure SQL Database

Microsoft Azure	,			
«	Inicio > Todos los recursos > conbbdd	- Control d	de acceso (IAM)	
+ Crear un recurso	Todos los recursos	« ×	ccnbbdd - Control de acceso (IAM) 30. Server	
A Inicio	+ Agregar ···	Más	, > Buscar (Ctr(+/)	
∃ Todos los servicios	CCNBBDD		Información general Comprobar acceso Asignaciones de roles Asignaciones de roles	
+ FAVORITOS			Registro de actividad	
Todos los recursos	🔍, ccnbbdd		Comprobar acceso Comprobar acceso Revise el nivel de acceso que tiene un usuario, un grupo, una	
🐑 Grupos de recursos				
Services			X Diagnosticar y solucionar pr Buscar 💿	
🦘 Function App			Configuración Usuario, grupo o entidad de servicio de Azure AD 🗸	
👼 SQL Database				
2 Azure Cosmos DR			Connected and the second section and	

4. Completar los siguientes campos.

Agrega	r asignación de roles	
Rol 🚯		
SQLADM	N	~
Asignar ac	ceso a 🕦	
Usuario, g	rupo o entidad de servicio de Azure	AD 💊
Selecciona	r O	
Administr	adores	
AS	Administradores SQL	
Miembros No se sele	seleccionados: ccionó ningún miembro. Busque y	agregue uno o vario
miembros	que quiera asignar ai roi de este r	ecurso.

- Rol: Seleccionar el nuevo rol.
- Asignar acceso: Usuarios, grupos o entidades de servicio de Azure AD.
- Seleccionar el grupo de Administradores SQL.
- 5. Para finalizar pulsar en [agregar].

Puede consultar los roles en la pestaña [Asignación de roles].



Guía de configuración segura para Azure SQL Database

🕂 Agregar 🛛 🔠 Editar columnas	👌 Actualizar 🔰 📋 Quita	r 💙 Got feedback?						
Comprobar acceso Asignacion	es de roles Asignaciones de de	negación Administradores clásicos	Roles					
Para administrar el acceso a los recursos de Azure de los usuarios, los grupos, las entidades de servicio y								
Nombre n		Rol	Ámbito n					
Busque por nombre o correo elec	Todo V	6 seleccionados V	Todos los ámbitos					
Agrupar por 🚯								
Rol V								
12 elementos (6 usuarios, 6 grupos)								
NOMBRE	TIPO	ROL						
AKS ADM USER								
US UsuariosADM_AKS	Grupo	AKS ADM User 👩						
AKS USER								
	_							
Us Usuarios_AKS	Grupo	AKS User 👩						
COLABORADOR DE SQL SERVER								
AS Administradores SQL	Grupo	Colaborador de SQL	Server 👩					
	_	-	-					

Nota: Esto es solo un ejemplo de la asignación de roles mediante **RBAC** los aplique desde el portal de Azure o los personalice.

Nota: Para una gestión más avanzada hay que recurrir al apartado [3.1.1.1 Requisitos de acceso/Control de acceso basado en roles] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.3 Segregación de funciones y tareas

Para la segregación de funciones y tareas se recomienda que se aplique un control de acceso basado en rol **(RBAC)** como se ha mencionado anteriormente ya que tiene varios roles integrados para recursos de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas.

Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure.

Si los roles integrados no cumplen las necesidades específicas de su organización, puede crear sus propios roles personalizados para los recursos de Azure.

A continuación, algunos ejemplos que puede aplicar para delegar las funciones y tareas.

1. Desde el portal de Azure pulsar en [grupo de recursos].



Guía de configuración segura para Azure SQL Database

Microsoft Azure	
«	Inicio > Grupos de recursos
+ Crear un recurso	Grupos de recursos
T Inicio	+ Agregar ≡≡ Editar columnas 🖒 Actualizar 🞍 Exportar a CSV 🛛 Ø Asignar etiquetas
⊨ Todos los servicios	Filtrar por nombre Suscripción == todo Ubicación == todo + Y Agregar filtro
+ FAVORITOS	Mostrando de 1 a 34 de 34 registros.
Todos los recursos	
😥 Grupos de recursos	CCN-RG-SQL
Redes virtuales	

2. Pulsar en [base de datos/Control de acceso (IAM)]



3. Pulsar en [Roles].



Nota: Desde esta pestaña puede ver todos los roles que puede asignar desde el portal de Azure.



Nota: Para una gestión más avanzada hay que recurrir al apartado [3.1.1.1 Requisitos de acceso/Control de acceso basado en roles] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

Nota: También se recomienda seguir el siguiente enlace de Microsoft https://docs.microsoft.com/es-es/azure/role-based-access-control/role-assignments-portal

3.1.1.4 Mecanismo de autenticación

Es importante destacar la integración de Azure Multi-Factor como un mecanismo seguro de autenticación. A su vez se recomienda crear una directiva de acceso condicional para los administradores de SQL.

Para ello, debe seguir estas directrices.

- 1. Desde el portal de Azure Pulsar en [Azure Active Directory]
- 2. Pulsar en [acceso condicional].



3. Pulsar en [nueva directiva].

Microsoft Azure		℅ Buscar recursos, servicios y documentos (G+/)				
«	Inicio >	eso condicional - Directivas				
+ Crear un recurso	Acceso condicional - Dire	ectivas				
🛧 Inicio	«	🕂 Nueva directiva 🛓 What If 🛛 🖤 ָTiene algún comentario?				
료 Panel	📜 Directivas	¿Le interesa comprender el impacto de las directivas en un inicio de sesión de usuario? Ec				
E Todos los servicios	Administrar					
+ FAVORITOS	↔ Ubicaciones con nombre	NOMBRE DE DIRECTIVA				
Todos los recursos	Controles personalizados (versi	Baseline policy: Require MFA for admins (vista previa) Baseline policy: End user protection (vista previa) Baseline policy: Block legacy authentication (vista previa)				
(Grupos de recursos	🧭 Términos de uso					
Services	conectividad VPN					
Function App	🚝 Directivas clásicas	Baseline policy: Require MFA for Service Management (vista previa)				
🕺 SQL Database	Solución de problemas y soporte	(
🖉 Azure Cosmos DB	técnico					
Máquinas virtuales						
💠 Equilibradores de carga	Solucional problemas					
🧮 Cuentas de almacenamiento	Nueva solicitud de soporte téc					
··· Redes virtuales						



- 4. En usuarios y grupos pulsar en seleccionar [usuarios y grupos].
- 5. Seleccionar Usuarios y grupos.
- 6. En el nuevo menú escribir y seleccionar Administradores SQL.
- 7. Para finalizar, pulsar en [aceptar].

A continuación, pulsar en [control de acceso].

Microsoft Azure			, P Buscar r	ecurso
«	Inicio > I - Company I - Company > Act	ceso condic	ional - Directivas > DirectivaSQL > Conceder	
+ Crear un recurso	DirectivaSQL	\times	Conceder	$ $ \times
Inicio Panel Todos los servicios	 Información Eliminar Nombre 	^	Seleccione los controles que deben exigirse.	
★ FAVORITOS	DirectivaSQL	- 1	Bioquear acceso Conceder acceso	
Todos los recursos	Tareas		Comprobación con MFA 🚯	
Grupos de recursos Or recursos Or recursos	Usuarios y grupos 🚯 Usuarios específicos incluidos	>	Requerir que el dispositivo esté marcado como compatible 🛛	
App Services	Aplicaciones en la nube o accio ① O aplicaciones en la nube selec	>	Requerir dispositivo unido a Azure A híbrido 🕐	'n
SQL Database	Condiciones () 0 condiciones seleccionadas	>	 Requerir aplicación cliente aprobada Ver la lista de aplicaciones cliente aprobadas 	-
Aquinas virtuales Aquinas de carga	Controles de acceso		Requerir directiva de protección de aplicaciones (versión preliminar) O Ver la lista de aplicaciones cliente	
🥃 Cuentas de almacenamiento	1 control seleccionado	>	protegidas por directivas	
 Azure Active Directory Monitor 	Sesión 🕐 O controles seleccionados	>	Para varios controles	
Asesor Security Conter	3 Habilitar directiva		Requerir todos los controles seleccionados	
 Administración de costos 	Activado Desactivado		Requerir uno de los controles seleccionados	

- 1. Seleccionar la casilla de comprobación MFA.
- 2. Pulsar en [aceptar].
- 3. Por último, pulsar en [guardar] para que se cree la nueva directiva.

Aparecerá la nueva directiva de acceso condicional para los usuarios Administradores de SQL. Esto fuerza a que el grupo de Administradores de SQL utilicen doble factor de autenticación.

Microsoft Azure		∠ Buscar recursos, servicios y documentos (G+/)				
×	Inicio > Acces	io condicional - Directivas				
+ Crear un recurso	Acceso condicional - Directory	ctivas				
🛧 Inicio	«	+ Nueva directiva 🔮 What If 🔰 🖤)Tiene algún comentario?				
🖽 Panel	š≣ Directivas					
∃ Todos los servicios	Administrar	U ¿Le interesa comprender el impacto de las directivas en un inicio de sesion de usuario/ Eche un vistazo a la herramienta "What IF. →				
+ FAVORITOS		NOMBRE DE DIRECTIVA				
Todos los recursos	Controles personalizados (versi	Baseline policy: Require MFA for admins (vista previa) Baseline policy: End user protection (vista previa) Baseline policy: Block legacy authentication (vista previa) Baseline policy: Require MFA for Service Management (vista previa)				
😭 Grupos de recursos	Tárminos de uso					
🔇 App Services						
Function App	ter conectividad verv					
🕺 SQL Database	3 Directivas clasicas					
🖉 Azure Cosmos DB	Solución de problemas y soporte	DirectivaSQL				
Máquinas virtuales	técnico					
Equilibradores de carga	🗙 Solucionar problemas					
Cuentas de almacenamiento	Nueva solicitud de soporte téc					



Es importante conocer los conceptos del acceso condicional ya que puede asignar diversas condiciones de autenticación.

Se pueden agregar distintas condiciones desde una directiva de acceso condicional. Atendiendo dispositivos autorizados, ubicaciones geográficas, rangos de ips, grupos de usuarios entre otros.

Nota: *Para una gestión más avanzada hay que recurrir al apartado* [3.1.1.1 Requisitos de acceso/Acceso condicional] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.2 Explotación

3.2.1 Registro de la actividad de los usuarios

El registro de actividad contiene todas las operaciones de escritura (PUT, POST, DELETE) para los recursos.

Los registros de actividad se conservan 90 días. Puede consultar cualquier intervalo de fechas, siempre que no hayan transcurrido más de 90 días desde la fecha inicial.

Mediante los registros de actividad, puede determinar:

- Qué operaciones se realizaron en los recursos en la suscripción.
- Quién inició la operación.
- Cuando tuvo lugar la operación.
- El estado de la operación.
- Los valores de otras propiedades que podrían ayudarle en la investigación de la operación.

Portal de Azure

- 1. Para ver los registros de actividad mediante el portal, pulsar en todos los recursos.
- 2. Pulsar en su [base de datos].

Microsoft Azure			
«	Inicio > Todos los recursos > c	cnbbdd - Registro d	de actividad
+ Crear un recurso	Todos los recursos	« ×	ccnbbdd - Registro de activio
A Inicio	🕂 Agregar	••• Más	Q Buscar (Ctrl+/)
🛄 Panel			
∃ Todos los servicios	Filtrar por nombre		🗟 Información genera
- 🛧 FAVORITOS	NOMBRE 1		Registro de actividad
Todos los recursos	↔ CCN-VNET-Backend	^	Control de acceso (IAM)
🐑 Grupos de recursos	···· CCN-VNET-Firewall		Etiquetas
↔ Redes virtuales	↔ CCN-VNET-Kubernetes		X Diagnosticar y solucionar pr
🔇 App Services	S CCN-VPN		Configuración
icación de funciones			🗳 Inicio rápido
🧟 SQL Database	💩 ccnbbdd		🌻 Grupos de conmutación por
Azure Cosmos DB			Administrar copias de seguri

3. En este panel encontrar varios filtros que puede aplicar.



CCN-STIC 884C Guía de configuraci

Microsoft Azure			P Buscar	recursos, servicios y documentos (G+/)		Ð	- G	P	® ?	٢	adm
«	Inicio > Todos los recursos > co	nbbdd - Registro	de actividad								
+ Crear un recurso	Todos los recursos	« ×	ccnbbdd - Registro de ac	tividad							
A Inicio	🕂 Agregar	••• Más	,O Buscar (Ctrl+/)	📰 Editar columnas O Actualizar 🔟 Exportar :	a Centro de eventos 🛛 🛓 🛙	Descargar como CSV 🤞	Registro	s 🗴	Anclar los	s filtros ac	tuales:
i≣ Todos los servicios	Filtrar por nombre		Información general	,O Buscar	X Onclusiones ra	ápidas					
+ FAVORITOS	NOMBRE 1.		Registro de actividad	Suscripción : CCN-STIC 823 Intervalo de tiemp	po : Últimas 6 horas	Gravedad del evento : Todos	. G	rupo de r	ecursos : CC	N-RG-SQ	L 0
Todos los recursos	> CCN-VNET-Backend	^	Control de acceso (IAM)	Recurso : ccnbbdd 🔹 🕇 🖓 Agregar filtro							
(🐑) Grupos de recursos	CCN-VNET-Firewall		🛷 Etiquetas	2 elementos.							
Redes virtuales	. CCN-VNET-Kubernetes		X Diagnosticar y solucionar pr	NOMBRE DE LA OPERACIÓN	ESTADO TIEMPO	MARCA DE TIE SUSCRIP	CIÓN				EVE
S App Services	S CCN-VPN		Configuración	Action taken as a result of Amira Dolini avail	Correcto Hace 4 horas	Thu See 26 CON-ST	10 833				8.41
Aplicación de funciones	CCN-VPNCONEXION		📣 Inicio rápido	Action taken as a result of Azure Policy eval	Correcto Habe 4 horas	ind sep 20 CCN-SI	10 623				MI
👼 SQL Database	acabbdd		Grupos de conmutación por	 Action taken as a result of Azure Policy eval 	Correcto Hace 4 horas	Thu Sep 26 CCN-ST	IC 823				Mi

4. Pulsar en [conclusiones rápidas] puede visualizar los eventos de las ultimas 24 hs. Así mismo, desde este panel, puede personalizar filtros de búsqueda de eventos.

Microsoft Azure			P Busca	recursos, servicios y documentos (G+/)	b 🗣 🔎 🚳 ? 😳
«	Inicio > Todos los recursos > conbbdd - R	Registro de a	ctividad		Conclusiones rápidas (últimas 24 horas)
+ Crear un recurso	Todos los recursos «	×	ccnbbdd - Registro de ac	tividad	
nicio	🕂 Agregar \cdots N	viás [,O Buscar (Ctrl+/)	🎫 Editar columnas 🐧 Actualizar 👔 Exportar a Centro de eventos 🛓 C	Errores Errores Errores Errores Errores Errores S
≡ Todos los servicios	Filtrar por nombre		Información general	🔎 Buscar 🗙 🤯 Conclusiones ră	
+ FAVORITOS	NOMERE 1.		 Registro de actividad 	Suscripción : 000 000000 Intervalo de tiempo : Últimas 6 horas	Implementaciones con errores
Todos los recursos	(++) CCN-VNET-Backend	··· ^ 4	Control de acceso (IAM)	Recurso : ccnbbdd 🔹 🐴 Agregar filtro	puede implementarios. 0
🗊 Grupos de recursos			🖗 Etiquetas	2 elementos.	
🐡 Redes virtuales	··· CCN-VNET-Kubernetes	3	X Diagnosticar y solucionar pr	NOMBRE DE LA OPERACIÓN ESTADO TIEMPO	Alertas activadas
S App Services	CCN-VPN	0	Configuración	▲ Action taken as a result of ∆zure Policy eval Correcto Hace 4 horas	Alerta de Azure que na activado un evento de activación de alertas. 0
🦘 Aplicación de funciones	CCN-VPNCONEXION		Inicio rápido	A defected on an include the order and demonstration of the order.	
👼 SQL Database	🐻 ccnbbdd	(Grupos de conmutación por	Action taken as a result of Azure Policy eval. Correcto. Hace 4 horas	A Service Health
🖉 Azure Cosmos DB		4	Administrar copias de seguri		afectar a una o varias de sus suscripciones.
👤 Máquinas virtuales			Administrador de Active Dire		

3.2.2 Protección de claves criptográficas

Azure SQL proporciona varios tipos de cifrado que ayudan a proteger información confidencial, como cifrado de datos transparente (TDE).

La clave de cifrado de datos simétrica se protege, además, cifrándose con una jerarquía de claves almacenadas en SQL Server.

En la imagen siguiente se compara la jerarquía de claves de administración y servicio tradicional con el sistema del Almacén de claves de Azure.



A continuación, se describen los pasos que se debe realizar para cifrar su base de datos utilizando Azure Key Vault.



- 1. Desde el portal de Azure pulsar en [todos los recursos].
- 2. Seleccionar su [base de datos].

Microsoft Azure		℅ Buscar recursos, servicios y documentos (G+/)	
«	Inicio > Todos los recursos		
+ Crear un recurso	Todos los recursos		
 Inicio Panel Todos los convisios 		♦ Asignar etiquetas	 Información de ve todo (€) (+ Agrega
	Mostrando de 1 a 1 de 1 registros.		
Todos los recursos	NOMBRE TU	TIPO 🛧	GRUPO DE RECURSOS
Grupos de recursos App Services	Cnbbdd	SQL Server	CCN-RG-SQL
🦘 Function App			

Pulsar en [cifrado de datos transparente].

Microsoft Azure			
«	Inicio > Todos los recursos > o	cnbbdd	
Crear un recurso	Todos los recursos	« ×	ccnbbdd
🛧 Inicio	- Agregar	••• Más	«
🖬 Panel	Agregat	1410.5	O Buscar (Ctrl+/)
∃ Todos los servicios	ccnbbdd		📣 Inicio rápido
★ FAVORITOS			Grupos de conmutación por
Todos los recursos	👼 ccnbbdd		Administrar copias de seguri
😭 Grupos de recursos			Administrador de Active Dire
🔇 App Services			🗟 SQL Database
Function App			Grupos elásticos de SQL
👼 SQL Database			👿 Bases de datos eliminadas
🖉 Azure Cosmos DB			- Historial de importación y ex
🕺 Máquinas virtuales			Cuota de DTU
💠 Equilibradores de carga			Propiedades
🥃 Cuentas de almacenamiento			
💮 Redes virtuales			Evportar plantilla
Azure Active Directory			
🕒 Monitor			Seguridad
👎 Asesor			Advanced Data Security
Security Center			🚺 Auditoría
Administración de costos			Firewalls y redes virtuales
Avuda v soporte técnico			Conexiones de puntos de co
Suscripciones			Cifrado de datos transparente

En este panel debe activa su propia clave, ya que utilizará Key Vault.

- 3. Pulsar en usar su propia clave.
- 4. Pulsar en seleccionar almacén de llaves.
- 5. Pulsar en crear un nuevo almacén. Deberá completar los siguientes campos.
 - Nombre: Definir el nombre que se va a utilizar para el nuevo almacén.
 - Suscripción: Seleccionar su suscripción.
 - **Grupo de recursos:** Se recomienda crear un nuevo grupo que estará dedicado para este Almacén. Solo le pedirá un nombre para definirlo.
 - Ubicación: Seleccionar Norte de Europa.

HELINIC Record of Seguridad		
-STIC 884C Guía de conf	iguración segura par	a Azure SQL Database
	Crear almacén	de claves \Box \times
	* Nombre 🗿	
	CCNKEY	√
	* Suscripción CCN-STIC 823	~
	* Grupo de recursos	
	CCN-RG-SQL Crear nuevo	~
	* Ubicación	
	Norte de Europa	<u> </u>
Inicio > Todos los recursos > ccnbbdd - Cifrado d	e datos transparente	
Todos los recursos « \times	ccnbbdd - Cifrado de dat	os transparente
🕂 Agregar 🛛 🚥 Más		开 Guardar 🛛 🗙 Descartar 🔍 Comentarios
ccnbbdd	Inicio rápido Grupos de conmutación por	Cifra sus bases de datos, copias de seguridad y registros en reposo sin realizar cambios en la 🛛 Z aplicación. Para habilitar TDE, hágalo en cada base de datos.
🚳 ccnbbdd \cdots	Administrar copias de seguri	Usar su propia clave 👩
	Administrador de Active Dire	Sí No
	SQL Database	Seleccionar una clave Indicar identificador de clave
	 Grupos elasticos de SQL Bases de datos eliminadas 	Key Vault
	Historial de importación y ex	Seleccionar un almacén de claves
	Cuota de DTU	* Tecla >
	Propiedades	
	Bloqueos	Hacer que la clave seleccionada sea el protector de TDE predeterminado.
	🛂 Exportar plantilla Seguridad	CU usa los permisos Get, Wap Key y Unurap Key para acceler a la Inacán de claves eleccimado. Etico permisos dos auxan para acceder al almacán de claves del TDE. Si es secesario, intentaremos concederle los permisos en su nombre.

6. Para finalizar pulsar en [guardar].

Nota: *Para una gestión más avanzada hay que recurrir al apartado* [3.1.2.4 Protección de claves] *de la guía.* [CCN-STIC-884A - Guía de configuración segura para Azure].

3.2.3 Monitorización del sistema

Log Analytics de Azure Monitor es una herramienta que se debe usar para obtener información detallada de los registros de Azure Monitor.

Para ello, debe seguir estas instrucciones de configuración:

1. Desde la base de datos de SQL pulsar en [Registro de actividad]



CCN-STIC 884C Guía de confi

Guía de configuración segura para Azure SQL Database

Microsoft Azure	
«	Inicio > ccnsql - Registro de actividad
+ Crear un recurso	ccnsql - Registro de actividad
1 Inicio	
🗔 Panel	
🗮 Todos los servicios	🗟 Información general
- 🔶 FAVORITOS	Registro de actividad
Todos los recursos	R Control de acceso (IAM) 4
😥 Grupos de recursos	Etiquetas
	Biognosticary colucionar pro

2. Después pulsar en [Registros].

Microsoft Azure		℅ Buscar recursos, servicios y documentos (G+/)
«	Inicio > ccnsql - Registro de actividad	
+ Crear un recurso	ccnsql - Registro de activi	dad
👕 Inicio		📰 Editar columnas 🕐 Actualizar 🛞 Diagnostics settings 🞍 Descargar como CSV 🥔 Registros 🔗
🗮 Todos los servicios	Información general	🔎 Buscar X 🔅 Conclusiones rápidas
+ FAVORITOS	Registro de actividad	Suscripción : Gravedad del evento : Todos Gravedad del evento : Todos Gravedad del evento : Todos
Todos los recursos	🙊 Control de acceso (IAM)	A elementor

3. Pulsar en [Agregar].

Microsoft Azure	P Buscar recurso
«	Inicio > ccnsql - Registro de actividad > Información general del análisis de los registros de actividad
+ Crear un recurso	Información general del análisis de los registros de actividad
1 Inicio	
🖽 Panel	
≡ Todos los servicios	Últimas 24 horas

4. Ahora aparece un asistente donde hay que crear un nuevo área de trabajo para los registros. Pulsar en [crear área de trabajo nueva].

Análisis de registros de activi \times $_{\rm Crear nueva solución}$	Áreas de trabajo de Log A $\Box~ imes$			
Área de trabajo de Log Analytics > Seleccione un área de trabajo	Crear área de trabajo nueva			

5. En el asistente identificar un nombre y un grupo de recursos. El grupo de recursos puede ser nuevo o elegir alguno existente. Se recomienda que sea un nuevo grupo.



CCN-STIC 884C Guía de configuración segura para Azure SQL Database

Crear nuevo Vincular existente	2
Área de trabajo de Log Analytics * 🛈	
AreaSQL	~
Suscripción *	
100-0100	~
Grupo de recursos *	
CCN-RG-SQL	\sim
Crear nuevo	
Ubicación *	
Norte de Europa	~
*Plan de tarifa	``

6. Para finalizar, pulse en [Aceptar].



Nota: *Este proceso puede tardar unos minutos.*

Al finalizar aparece un nuevo panel.

Microsoft Azure			
«	Inicio > ccnsql - Registro de actividad > Información genera		
+ Crear un recurso	Información general del análisis de los regis		
🏫 Inicio			
⊡ Panel			
🗮 Todos los servicios	Últimas 24 horas		
★ FAVORITOS	Filtrar por nombre		
Todos los recursos			
😥 Grupos de recursos	AzureActivity(AreaSQL)		
↔ Redes virtuales	Realizando evaluación		
📀 App Services	To use this solution, please connect an Azure Subscription for		
🦘 Aplicación de funciones	collecting activity logs. A subscription can be connected using the activity logs blade of a workspace in the Azure		
🧧 SQL Database	portal.		
S Azure Cosmos DB			

Importante: En el momento que se crea esta nueva área. Puede tardar un tiempo en la recolección de logs.

Un ejemplo gráfico.



84C Guía de configuración segura para Azure SQL Database

ACTIVITY LOGS BY RESOURCE PROVIDER					
Resource providers producing activity logs					
10					
IU					
RESOURCE PROVIDER	COUNT				
Microsoft.Compute	340				
Microsoft.Storage	178				
Microsoft.RecoveryServices	42 🗖				
Microsoft.ContainerService	28 🔳				
Microsoft.Authorization	10 I				
Microsoft Resources	20 🔳				
Microsoft.Network	55 🗖				
Microsoft.DevSpaces	4 1				
Microsoft SQL	91				
	4.1				

Microsoft Azure		𝒫 Buscar recursos, servicios y documentos (G+,/)			> 🗣 🗳 🐵
«	Inicio > ccnsql - Registro de actividad > Info	rmación general del análisis de los registros de actividad > AzureActivity(CCN-RG-Log) > Regis	itros		
+ Crear un recurso	Registros				
T Inicio	PNueva cons * +			🛄 Ayuda	a 👸 Configuración 🗄 Consi
≡ Todos los servicios	CCN-RG-Log Seleccionar ámbito	Ejecutar Intervalo de tiempo : Últimos 7 días		📙 Guard	dar 🕲 Copiar 🛏 Exportar –
FAVORITOS Todos los recursos Grupos de recursos	Esquema Filtrar «	AzureActivity where ResourceProvider == "Microsoft SQL" // Oql: Type-AzureActivity ResourceProvider == "Microsoft SQL" // Sett	ings: {NAV: True} //	WorkspaceId: {00000	809-8089-8089-8889-88888
Redes virtuales App Services Aplicación de funciones	F= Contraer todo Activo ▼				
SQL Database	LogManagement NetworkMonitoring	Completado. Showing results from the últimos 7 días.			
Máquinas virtuales	SecurityCenterFree	Drag a column header and drop it here to group by that column			
Equilibradores de carga	 fx Funciones 	TimeGenerated (Bruselas, Copenhague, Madrid, Paris) ↓ ∇ OperationName	Level	ActivityStatus V	ActivitySubstatus 🗸
Cuentas de almacenamiento	Áreas de trabajo favoritas	14/11/2019 15:00:35:335 Create/Update Database Backup	Archival Policy Information	nal Succeeded	
Azure Active Directory		> 14/11/2019 15:00:17.929 Create/Update Database Backup	Archival Policy Information	nal Accepted	Accepted (HTTP Status Code: 202)
🕑 Monitor		> 14/11/2019 15:00:17.924 Updates a short term retention p	olicy Information	nal Accepted	Accepted (HTTP Status Code: 202)
🐢 Asesor		> 14/11/2019 15:00:17.718 Updates a short term retention p	olicy Information	nal Started	
Security Center		> 14/11/2019 15:00:17.708 Create/Update Database Backup	Archival Policy Information	nal Started	
O Administración de costos		> 14/11/2019 14:52:23.613 Create/Update Database Backup	Archival Policy Information	nal Succeeded	
Ayuda y soporte técnico		14/11/2019 14:52:08.011 Create/Update Database Backup 14/11/2019 14:52:07.821 Create/Update Database Backup	Archival Policy Information Archival Policy Information	nal Accepted	Accepted (HTTP Status Code: 202)

Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.6Monitorizacion de sistema] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.3 Medidas de protección

3.3.1 Protección de las comunicaciones

3.3.1.1 Perímetro seguro

Existe una separación de los roles de seguridad en la administración de puntos de conexión de servicio de red virtual. Se requiere una acción de cada uno de los roles siguientes:

Existen dos niveles.



1. Reglas nivel base de datos individuales.

Estas reglas permiten a los usuarios acceder a determinadas bases de datos (seguras) dentro del mismo servidor de SQL Database. Debe crear estas reglas para cada base de datos y se almacenan en las bases de datos individuales.

2. Reglas nivel servidor.

Estas reglas permiten a los usuarios obtener acceso a toda la instancia de Azure SQL Server (es decir, a todas las bases de datos que se encuentren en el mismo servidor de SQL Database). Estas reglas se almacenan en la base de datos **principal**. Las reglas de firewall de IP de nivel de servidor.

Nota: Es importante saber que esta regla de firewall aplica específicamente a las comunicaciones de las bases de datos.

A continuación, ejecutar estos comandos mediante PowerShell:

1. Creación de regla nivel base de datos individuales en SQL.

```
# EXECUTE sp_set_database_firewall_rule N'Example DB
Rule','0.0.0.4','0.0.0.4';
```

2. Creación de regla de firewall indicando el rango de ip origen y destino para que se apliquen en el servidor.

Existen otros tipos de recomendaciones para el aislamiento de la base de datos, así como la configuración de Azure firewall y NSG.

Nota: Para esta gestión más avanzada, hay que recurrir al apartado [3.2.1 Proteccion de las comunicaciones/3.2.1.2 Perímetro seguro] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.3.2 Protección de la información

3.3.2.1 Calificación de la información

Para la clasificación de la información se recomienda el uso de etiquetas.

Se componen de clave-valor definidos por el usuario, se pueden colocar directamente en un recurso o un grupo de recursos.

Actualmente, Azure admite un máximo de 15 etiquetas por recurso y grupo de recursos.

Las etiquetas se pueden colocar en un recurso en el momento de su creación, o bien se pueden agregar a un recurso existente.

En Azure SQL se recomienda el uso de estas etiquetas que se deben emplear en las máquinas virtuales, grupo de recursos, base de datos.



CCN-STIC 884C Gu

Nota: Para para conocer más el uso de etiquetas y su configuración hay que recurrir al apartado [3.2.2 Protección de la información/3.2.2.1 Clasificación de la información] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.3.2.2 Copias de seguridad (backup)

Existen distintos métodos desde Azure para realizar backups. En este caso debe utilizar como primera medida una retención de su base de datos.

A continuación, se describe las instrucciones que debe seguir para configurar la retención en sus bases de datos.

1. Desde el portal de Azure pulsar en [Grupo de recursos]

Microsoft Azure					
	~				
+ Crear un recurso					
🟫 Inicio					
⊡ Panel					
Todos los servicios					
+ FAVORITOS		÷			
Todos los recursos					
💽 Grupos de recursos					
Redes virtuales					
📀 App Services					
🦘 Aplicación de funciones					
ब SQL Database					
🧕 Azure Cosmos DB					
Máquinas virtuales					

2. Pulsar en el grupo de recursos donde se encuentra su base de datos.

MICrosoft Azure	Discorrecursos, se
«	Inicio > Grupos de recursos
+ Crear un recurso	Grupos de recursos
숨 Inicio	+ Agregar ≣≣ Editar columnas () Actualizar ↓ Exportar a CSV Ø Asignar etiguetas C
🗔 Panel	
≡ Todos los servicios	Filtrar por nombre Suscripción == todo Ubicación == todo Image: Transmission of the second
+ FAVORITOS	Mostrando de 1 a 36 de 36 registros.
Todos los recursos	□ Nombre ↑↓
😥 Grupos de recursos	CCN-RG-RECOVERY
Redes virtuales	CCN-RG-SQL
App Services	CCN-RG-VMs
Aplicación de funciones	CCN-RG-VMs-asr
-	

3. Pulsar en su base de datos y después pulsar en Administrar copias de seguridad.



CCN-STIC 884C Guí

Guía de configuración segura para Azure SQL Database



4. Pulsar en [Configurar retención].

Microsoft Azure	P Buscar recursos, servicios y documentos (G+/)
«	Inicio 🗧 consql - Administrar copias de seguridad
+ Crear un recurso	Ccnsql - Administrar copias de seguridad
🟫 Inicio	Configurar directivas Copias de seguridad disponibles
🖽 Panel) Buscar (Ctrt+/)
🗮 Todos los servicios	🗟 Información general 🔷 🖉 Configurar retención 🚫 Quitar configuración 🖒 Actualizar ♡ Comentarios
+ FAVORITOS	Registro de actividad Puede configurar directivas de retención de copias de seguridad en varias bases
Todos los recursos	⁸ Control de acceso (IAM)
🧭 Grupos de recursos	Etiquetas P Buscar para filtrar bases de datos

5. Se abre una nueva ventana donde debe completar la siguiente información.



CCN-STIC 884C Guía de con

Guía de configuración segura para Azure SQL Database

Configurar directivas SQL Server	>
Configuración de restauración a un momento dad	0
7 Vias	
Configuraciones de retención a largo plazo	
Copias de seguridad de LTR semanales ()	
¿Durante cuánto tiempo quiere que se conserven las c	opias de seguridad semanales?
1 🗸 Año	s) 🗸
Copias de seguridad de LTR mensuales ① ¿Durante cuánto tiempo quiere que se conserve la priv	nera copia de seguridad de cada mes?
Copias de seguridad de LTR anuales 🛈	·
¿Qué copia de seguridad semanal del año quiere cons	ervar?
Semana 1 🗸 🗸	
¿Durante cuánto tiempo quiere que se conserve esta o	opia de seguridad anual?
1 Año	5) 🗸

- Configuración de restauración a un momento dado: Dispone
- Configuración de retención a largo plazo: Dispone de 7 a 35 días.
- Copias de seguridad de LTR mensuales: Debe asignar el tiempo que se conserven las copias de seguridad semanales
- **Copias de seguridad de LTR anuales**: Puede seleccionar desde 1 semana hasta 52 semanas al año.
- 6. Una vez definida la configuración pulse en [Aplicar]

Puede consultar más información en el enlace https://docs.microsoft.com/es-es/azure/sql-database/sql-database-automated-backups

Nota: Para una gestión más avanzada hay que recurrir al apartado [2.3 Gestión de recursos Azure/Grupo de recursos] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].

3.4 SCRIPTS DE CONFIGURACIÓN

Se adjunta el script formato JSON para la creación de un nuevo rol personalizado PaaS en los administradores de SQL.

Puede consultar sobre mas roles en los siguientes links.

- https://docs.microsoft.com/da-dk/azure/sql-database/sql-database-managelogins?toc=/azure/sql-data-warehouse/toc.json
- https://docs.microsoft.com/es-es/sql/relationaldatabases/security/authentication-access/application-roles?view=sql-serverver15



 https://docs.microsoft.com/es-es/sql/relationaldatabases/security/authentication-access/database-level-roles?view=sqlserver-ver15

4. GLOSARIO Y ABREVIATURAS

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

Término	Definición
AAD	Azure Active Directory (Directorio Activo de Azure).
AD DS	Active Directory Domain Services (Servicios de dominio de Directorio Activo).
Grupo de Recursos	contenedor que almacena los recursos relacionados con una solución de Azure. El grupo de recursos incluye los recursos que se desean administrar como grupo.
Azure AD	Azure Active Directory.
RBAC	RBAC es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.
JSON	Acrónimo de JavaScript Object Notation, «notación de objeto de JavaScript») es un formato de texto sencillo para el intercambio de datos.
ENS	Esquema Nacional de Seguridad.
MFA	Multifactor Authentication (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una app, sms, etc.
Log Analytics	Azure Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA) o agente Linux de OMS, se desarrolló para lograr una administración completa en las máquinas locales, en los equipos que supervisaba System Center Operations Manager y en las máquinas virtuales de cualquier nube. Los agentes de Windows y Linux se asocian a Azure Monitor y almacenan los datos de registro recopilados de diferentes orígenes en el área de trabajo de Log Analytics.
Cifrado de datos	El Cifrado de datos transparente (TDE) cifra los archivos de datos de SQL Server, Base de datos SQL de Azure y Azure Synapse



transparente	Analytics (SQL DW), lo que se conoce como cifrado de datos en
	reposo.



CCN-STIC 884C Guía de configuración segura para Azure SQL Database

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización puede valorar qué medidas de las propuestas se cumplen.

Control ENS	Configuracion	Estado)
ор	Marco Operacional		
op.acc	Control de Acceso		
op.acc.1	acc.1 Identificación		
	Se ha configurado el uso de cuentas y grupos de Azure Active directory para la administración del Tenant.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	



op.acc.2	Requisitos de Acceso		
	Se ha configurado el requisito tratados en el punto 3.1.1.4.	Aplica:	Cumple:
		🗌 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
op.acc.3	Segregación de funciones y tareas		
	Se han diseñado, creado y aplicado los roles a los grupos de usuarios. Mínimo han de aplicarse los roles Propietario, colaborador, lector y Administrador de acceso de usuario y administradores de bases de datos SQL, siguiendo la referencia de la guía de configuración segura de Azure.	Aplica:	Cumple:
		🗆 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	



op.acc.5	Mecanismo de autenticación		
	Se ha habilitado <u>Multi-Factor Authentication</u> (MFA) para los usuarios administradores de SQL utilizando una directiva de acceso condicional.	Aplica:	Cumple:
		🗌 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	
op.exp	Explotacion	'	
op.exp.8	Registro de la actividad de los usuarios		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos habilitando una nueva área de trabajo.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	



Op-exp.11	Protección de claves criptográficas		
	Se ha configurado Key Vault, límitando el acceso tan sólo a usuarios administradores. Siguiendo las instrucciones de la guia CCN-STIC-884A Configuración segura para Azure, apartado. [3.2.2.2 Cifrado]	Aplica:	Cumple:
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
Op.mon	Monitorizacion de sistema		
Op.mon.2	Sistema de métricas		
	Se ha configurado Azure monitor aplicando los registros populares haciendo referencia a las recomendaciones de Azure SQL Database.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No



		Evidencias Recogidas:	Observaciones:
		🗆 Si 🗌 No	
Mp.com.1	Perímetro seguro		
	Se ha configurado el acceso restringido utilizando reglas de firewall.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
Mp.info.2	Clasificacion de la informacion	'	
	Se han configurado etiquetas para diferenciar los servicios que compone las bases de datos de SQL, Maquinas virtuales, grupos de recursos.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No



		Evidencias Recogidas:	Observaciones:
		🗆 Si 🗌 No	
Mp.info.9	Copias de seguridad		
	Se ha configurado un politica de retencion de copias de seguridad.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	