

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0071/S005
Referencia - Reference: ES007100501545666
Fecha de validez – Valid until: 11/29/2025

Proveedor de servicio / Service provider

INTERNATIONAL BUSINESS MACHINES,
S.A.

Identificación del servicio calificado/ Rated Service identification

Familia de soluciones IBM Cloud® Databases/
IBM Cloud® Databases family of solutions

Descripción del servicio calificado / Rated service description

The commercial offering including in this service is the following:

Service	Description	Documentation link
IBM Cloud databases for MySQL	IBM Cloud® Databases for MySQL fully managed service ensures predictable performance, on-demand scaling, and robust security.	https://www.ibm.com/products/databases-for-mysql
IBM Cloud Databases for PostgreSQL	IBM Cloud® Databases for PostgreSQL is a fully managed service enabling you to efficiently create sophisticated, high-performance applications with enhanced JSON support and improved query parallelism	https://www.ibm.com/products/databases-for-postgresql

Alcance / Scope

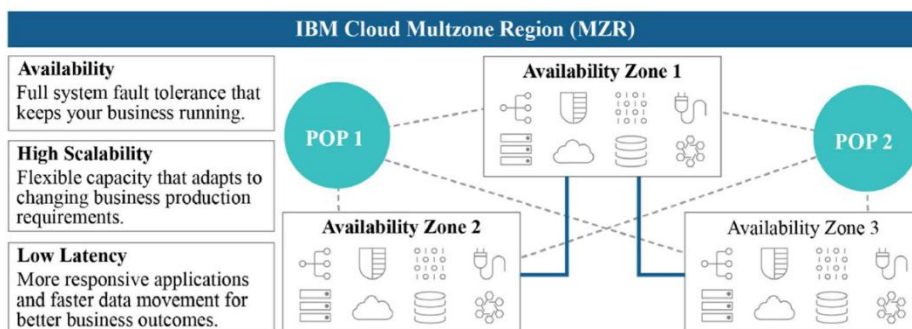
VPC COMMON INFRASTRUCTURE

IBM Cloud's heritage began with a focus on deployment of secure and isolated computing, and today our infrastructure services leverage next-generation capabilities built from the ground-up on Kubernetes. Cloud native technologies and global Site Reliability Engineering (SRE) best practices have been used to create “available at the click of a button” capabilities from infrastructure to platform to software services.

As a provider uniquely oriented toward regulated industry needs, IBM Cloud is focused on continuous compliance, operational excellence, and broad and pervasive data protection. IBM's clients leverage built-in fail-over at the infrastructure and platform levels to provide resiliency. They leverage data, AI, and analytics capabilities to monitor risk and transform business processes. Security, data protection, performance, resiliency, and availability are primary design considerations, amongst other industry leading features described throughout this document.

The Multi-Zone Region (MZR) model increases system availability through redundancy, while decreasing latency through the proximity of Data Centers (DCs) within the region to meet our customers' need for High Availability (HA). Each MZR includes multiple DCs to provide geographically redundant services.

IBM Cloud allows users to deploy workloads with the highest level of data protection at rest and in transit with Keep Your Own Key (KYOK), and seamless integration across IaaS and PaaS. In addition, industry-informed controls enable users, to operate securely with sensitive data in the public cloud. IBM Cloud's industry-informed controls allow our clients to enable the level of transparency and compliance required to modernize and accelerate mission-critical applications.



Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0071/S005
Referencia - Reference: ES007100501545666
Fecha de validez – Valid until: 11/29/2025

IBM Cloud is built on a hyperscale commercial cloud platform with IaaS, PaaS, and SaaS designed to provide enterprises with secure, open, high performance cloud capabilities. IBM Cloud offers a robust Red Hat OpenShift (Kubernetes) cloud platform, allowing customers to seamlessly develop, deploy, manage, and operate their workloads in IBM Cloud with full interoperability.

IBM Cloud Secure Virtualization together with IBM Cloud Virtual Private Cloud (VPC) provides logical separation, which is critical for regulated industry customers.

VPC DATA CENTERS WITHIN BOUNDARY AND SCOPE

IBM Cloud PaaS and VPC IaaS services are housed in IBM data centers that have implemented all necessary security measures to satisfy the ENS High controls described in this document. Data center operations create and manage physical infrastructure resources.

IBM Cloud services in scope for ENS High are available in multiple zones across one or more IBM Cloud regions. These are linked using multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management.

Application providers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities house both co-location servers and IaaS related servers. Co-location customers do not have logical or physical access to the infrastructure system. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

Locations and Vendors

Refer to the table below for a list of specific data centers and the associated vendors that provide facility management services in the IBM Cloud facilities within the boundaries of the system.

Facility	Physical Location	Facility Manager
MAD02	Madrid, ES	Data4
MAD04	Madrid, ES	NTT
MAD05	Madrid, ES	Interxion

Databases

In cloud native applications, it is typical to store application data in a database that is operated as a Database-as-a-Service by a cloud provider (although users can deploy their own databases on IBM Cloud, if they prefer). IBM offers a number of database technologies as a service, for example, Cloudant, which use native database encryption to provide encryption by default using an HSM-stored randomly generated key. These encrypt at the table level, and can be configured to use customer provided keys via KYOK or BYOK. IBM Cloud Databases use a similar replication model to IBM COS where databases are triple replicated across user specified region(s).

IBM recognizes that customer data resides in multiple places and in multiple forms in IBM Cloud. As such, IBM provides consistent key management and protection of data in all forms and locations, and while in motion as summarized in table below.

Proceso de calificación

El proceso de calificación consta de cuatro etapas:

- Elaboración de la memoria justificativa por parte del proveedor del servicio o realización de auditoría de tercero independiente conforme a la norma internacional ISAE 3402

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0071/S005
Referencia - Reference: ES007100501545666
Fecha de validez – Valid until: 11/29/2025

- Pre-evaluación documental de la memoria justificativa (o del informe de auditoría) y solicitud, en caso de que sea necesario, de subsanación de errores y/o aclaraciones
- Evaluación *in situ* de una muestra de controles incluidos en la memoria justificativa (solo en caso de que no se haya realizado auditoría previa)
- Elaboración de informe final y emisión del sello con la calificación obtenida

Una vez obtenido el sello, se ponen en funcionamiento los mecanismos de supervisión del esquema:

- Canal de incidencias
- Monitorización en fuentes abiertas
- Auditorías aleatorias

Este nivel de calificación se obtiene sobre la base de las respuestas indicadas por el proveedor de servicios en cuanto a la aplicabilidad y, en su caso, existencia de los controles incluidos en la metodología de calificación en su versión 3.1 y las evidencias aportadas por el mismo u obtenidas por el equipo de la agencia durante la revisión *in situ* en las instalaciones del proveedor del servicio.

Rating process

Rating and certification process have four steps:

- Preparation of a memory by the service provider or conducting an audit by an independent third party according to ISAE 3402.
- Documentary pre-assessment based on previous memory (or audit report) and require, if needed, correction or errors and/or clarifications.
- In situ assessment based on a sample of controls included in the memory.
- Preparation of final report and issue of the label and certification with the rating level obtained.

Once the label has been issued, supervision mechanisms come into place:

- Incident channel
- Cybersecurity online monitoring
- Random exhaustive audits

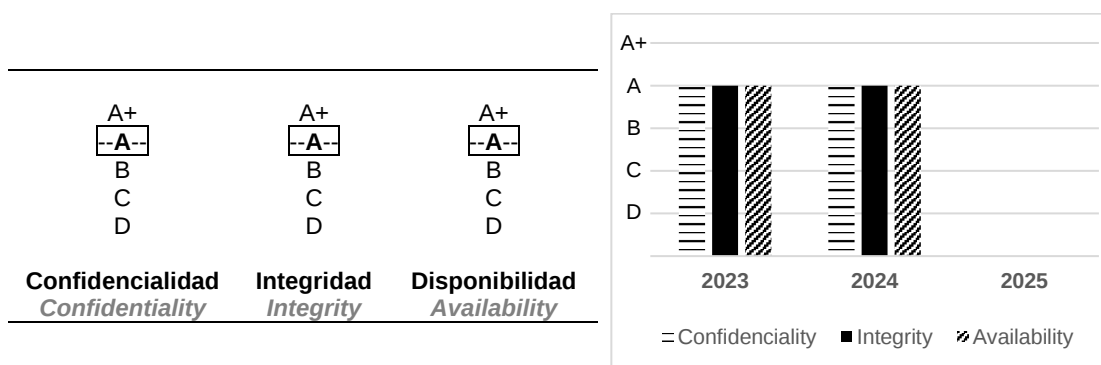
This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in rating methodology version 3.1 and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

Calificación

El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

Rating

The rating level obtained by the service and the comparison with previous years according to the qualification level after the aforementioned rating process has been carried out are the following:





CyberSecurity
Rating Agency

Nivel de garantía
Level of assurance



Certified in EU

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0071/S005
Referencia - Reference: ES007100501545666
Fecha de validez – Valid until: 11/29/2025

Los criterios para asignar la calificación global, según se establece en la versión 3 de la metodología son, implantar:

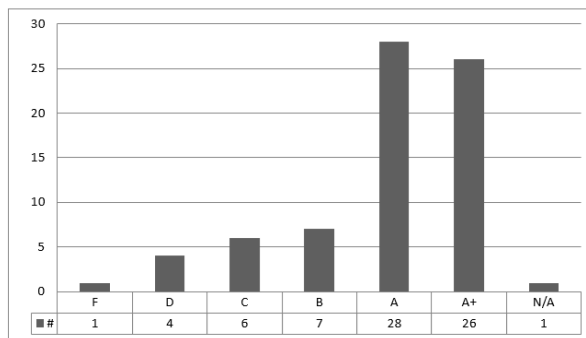
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que más contribuyen a una seguridad más ágil).

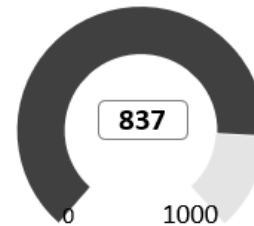
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- 100% of the general measures and for the corresponding dimension of priority '1'.
- At least 85% of the general measures and for the corresponding dimension of priority '2'.
- At least 50% of the general measures and for the corresponding dimension of priority '3'.

The evaluation of individual sections considers 100% of the controls (regardless of their priority) and it is showed in the following diagram. Quantitative rating is a weighted sum (base thousand) of levels achieved by sections (with a higher weight of those with a closer relation to agile security).



Calificación cuantitativa /
Quantitative Rating



Madrid, 10/17/2024



CyberSecurity
Rating Agency

D. Oscar Colado
Rating Evaluation Team – Operations Direction
Chief Auditor: Elena Miguel

Cliente/Servicio – *Client/Service*: ES0071/S005
Referencia - *Reference*: ES007100501545666
Fecha de validez – *Valid until*: 11/29/2025

ANEXO / ANNEX

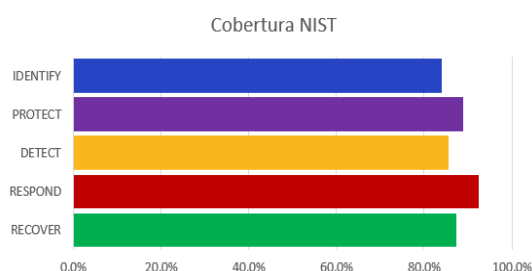
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES *INTERNATIONAL STANDARDS COVERAGE*

Cobertura respecto a NIST

Este gráfico muestra el porcentaje de implementación de las prácticas aplicables en el servicio, para el nivel objetivo evaluado (barra decolorada) y con respecto al nivel máximo (barra de color intenso), por cada una de las cinco etapas del marco de ciberseguridad del National Institute of Standards and Technology (NIST)¹.

NIST coverage

This chart shows the implementation porcentaje of practices applicable in the service, for the goal level reviewed (discolored bar) and for the maximum level (intense bar) in each of the five steps of NIST Cybersecuerity Framework.



Cobertura respecto a CIS

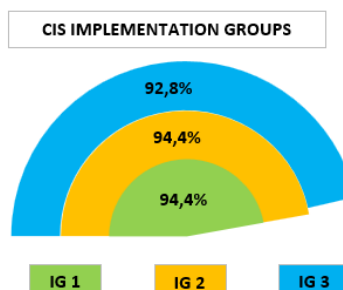
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 7² están divididos en tres grupos: *Basic*, *Foundational* y *Organizational*, que a su vez se clasifican en tres grupos de implementación: IG 1, IG 2 e IG 3, según el nivel de exigencia en seguridad que se marque la propia organización. El siguiente diagrama muestra su grado de implementación en el servicio evaluado.

CIS coverage

Center for Internet Security (CIS) collects and publishes the defense practices for most common attacks, known as CIS Controls.

The 20 controls of versión 7 are divided in three groups: Basic, Foundational and Organizational, that are also classified in three implementaton groups: IG1, IG2 and IG3 in growing order of demand. Following chart shows the implementation grade in the service in scope.



¹ <https://www.nist.gov/cyberframework>

² <https://www.cisecurity.org/controls/v7>



CyberSecurity
Rating Agency



Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0071/S005
Referencia - *Reference*: ES007100501545666
Fecha de validez – *Valid until*: 11/29/2025

INFORMACIÓN ANALÍTICA DE SU EVALUACIÓN *ANALYTIC INFORMATION OF YOUR RATING*

Resultado por áreas

Los controles han sido clasificados según los principios de *security economics* lo que permite obtener los gráficos siguientes con el porcentaje de implementados por cada tipo respecto al nivel evaluado como objetivo.

Results by areas

Controls have been classified according to security economics principles which allows getting the attached diagram showing the percentage of practices implemented in relation to those required by your goal level.

