Cliente/Servicio – *Client/Service*: **ES0071/S002**
Referencia - *Reference*: **ES007100203582133**
Fecha de validez – *Valid until*: **Nov/29/2026**

Proveedor de servicio / *Service provider*

International Business Machines SA

Identificación del servicio calificado/ ***Rated Service identification***

Familia de soluciones IBM Cloud® Virtual Private Cloud (VPC) /
IBM Cloud® Virtual Private Cloud (VPC) 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 Container Registry	Provides a multi-tenant, highly available, scalable, and encrypted private image registry hosted and managed by IBM.	(https://cloud.ibm.com/docs/Registry)
IBM Cloud Continuous Delivery	Built on Open Toolchain, it enables automated continuous integration and delivery of cloud-native apps on Kubernetes.	(https://cloud.ibm.com/docs/ContinuousDelivery)
IBM Cloud Event Notifications	Routes critical event information or triggers automated actions using webhooks.	(https://cloud.ibm.com/docs/event-notifications)
IBM Cloud Kubernetes Service (on VPC)	Managed service for creating Kubernetes clusters to deploy and manage containerized apps.	(https://cloud.ibm.com/docs/containers)
Red Hat OpenShift on IBM Cloud (on VPC)	Deploy apps on highly available OpenShift clusters running on IBM Cloud Container Platform.	(https://cloud.ibm.com/docs/openshift)
IBM Cloud Object Storage	Stores encrypted and dispersed data across multiple geographic locations.	(https://cloud.ibm.com/docs/cloud-object-storage)
IBM Cloud Identity and Access Management (IAM)	Enables secure user authentication and access control across IBM Cloud resources.	(https://cloud.ibm.com/docs/account)
IBM Cloud Satellite	Extends public cloud scalability and flexibility to secure private cloud environments.	(https://cloud.ibm.com/docs/satellite)
IBM Cloud Schematics	Delivers Infrastructure as Code (IaC) tools as a service.	(https://cloud.ibm.com/docs/schematics)
IBM Cloud Security and Compliance Center (SCC)	Provides tools to secure, comply, and manage containerized workloads with a CNAPP solution.	(https://cloud.ibm.com/docs/security-compliance)
IBM Cloud Secrets Manager	Create, lease, and centrally manage secrets using HashiCorp Vault-based instances.	(https://cloud.ibm.com/docs/secrets-manager)
IBM Event Streams for IBM Cloud (Enterprise)	High-throughput message bus built with Apache Kafka.	(https://cloud.ibm.com/docs/EventStreams)

IBM Key Protect for IBM Cloud	Full-service encryption solution using envelope encryption and FIPS 140-2 Level 3 certified HSMs.	(https://cloud.ibm.com/docs/key-protect)
IBM Cloud Virtual Private Cloud - Private Paths for VPC	Private Path services provide private connectivity for IBM Cloud and third-party services. Traffic stays on the IBM backbone without traversing the internet.	https://test.cloud.ibm.com/docs/vpc?group=private-path-services
IBM Managed Dedicated Storage Cluster	IBM Managed Dedicated Storage Cluster is a 2-zone file service based on NetApp's MetroCluster synchronous replication solution. IBM will provide dedicated hardware, including daily maintenance, patch updates, and data center operations responsibilities	https://test.cloud.ibm.com/docs/ssad?topic=ssad-systems-services-architecture-for-dedicated-storage-cluster

Alcance / *Scope*

IBM Cloud VPC

VPC is a public cloud offering that lets an enterprise establish its own private cloud computing environment on shared public cloud infrastructure. A VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private, secure place on the public cloud. Physical compute separation is also possible via dedicated nodes.

VPC provides users with secure and scalable infrastructure resources, including software defined network constructs, compute instance types as virtualized infrastructure, and storage primitives. VPC is advantageous to users who have requirements to provision infrastructure components for performance or isolation reasons, or who provide advanced cloud services to other users on top of infrastructure primitives. Users can provision storage, compute instances, and software defined networks via user interface (UI), CLI, or representational state transfer (REST) API.

VPC users have two options for compute:
• IBM Cloud™ Virtual Servers for Virtual Private Cloud - An Infrastructure-as-a-Service (IaaS) offering that gives access to all the benefits of VPC, including network isolation, security, and flexibility. With Virtual Servers for VPC, a user can quickly provision instances with high network performance. When a user provisions an instance, they can select a profile that matches the amount of memory and compute power needed for the application that will run on that instance. Instances are available on the x86 architecture. After provisioning an instance, the user can control and manage those infrastructure resources.

• Red Hat® OpenShift® on IBM Cloud - Managed offering to create an OpenShift cluster of compute hosts to deploy and manage containerized apps on IBM Cloud. Red Hat OpenShift on IBM Cloud provides intelligent scheduling, self-healing, horizontal scaling, service discovery and load balancing, automated rollouts and rollbacks, and secret and configuration management for apps. Combined with an intuitive user experience, built-in security and isolation, and advanced tools to secure, manage, and monitor cluster workloads, a user can rapidly deliver highly available and secure containerized apps in the public cloud.

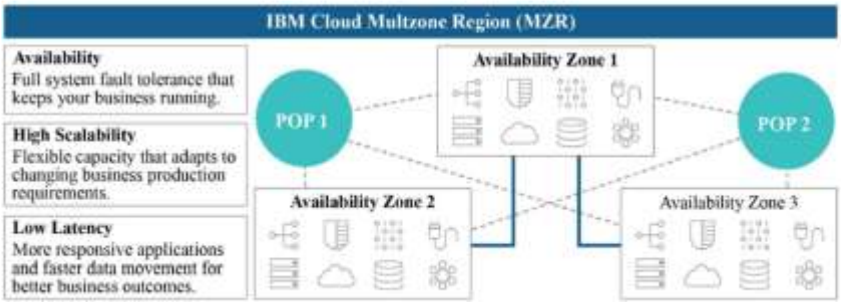
VPC COMMON INFRASTRUCTURE

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.


IBM Cloud Multzone Region (MZR)
Availability
Full system fault tolerance that keeps your business running.
High Scalability
Flexible capacity that adapts to changing business production requirements.
Low Latency
More responsive applications and faster data movement for better business outcomes.
POP 1
Availability Zone 1
POP 2
Availability Zone 2
Availability Zone 3

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
FRA02*	Frankfurt, DE Leonhard - Heisswolf Str 4.Frankfurt am Main, 65936 DE, Germany	Cyrus One
FRA04	Frankfurt, DE Eschborner Landstrasse 100, Frankfurt, Germany	NTT Data
FRA05	Frankfurt, DE Weissmullerstrasse 40 Frankfurt, Germany	Digital Realty
MAD02*	Madrid, ES Av. de la Industria, 15, 28108 Alcobendas, Madrid, Spain	Data4
MAD04	Madrid, ES C. Aquisgrán, 2, 28232 Las Rozas de Madrid, Madrid, Spain	NTT Data
MAD05	Madrid, ES C. de Alfonso Gómez, 6, 28037 Madrid, Spain	Digital Realty
PAR01	Paris, FR 7-9 rue Petit - 92582 Clichy, France	Global Switch
PAR04	Paris, FR 7-9 rue Petit, 92582 Clichy, France	Global Switch
AMS03	Amsterdam, AMS Rondebeltweg 62, Almere, 1329BG, The Netherlands	NorthC Datacenters Almere
MIL01	Milan, MIL Via Monzoro 101-105 20010 Cornaredo (MI), Italy	Data4

(*) Two data centers that have been included in the audit sample.

VPC environments

IBM uses Terraform and Ansible open-source software, which enable predictable and consistent provisioning of cloud resources. Terraform can also be used to configure and automate cloud resource provisioning across cloud providers. As users deploy assets and begin to build infrastructure, library templates may be utilized to speed progress. These templates establish standard configurations of network access, security, performance, and other configuration settings. Users may further customize ACLs, security, or network settings by running Windows or Linux consoles, saving the configuration file in IBM Cloud as a deployment pattern for their account.
Alternatively, users can have workloads securely hosted within Docker containers and managed via Red Hat OpenShift or Kubernetes container management systems. The container image can be preconfigured for high security so that workloads are deployed in a way that meet additional security

requirements. Containers and container contents (including metadata and code) may be encrypted to protect data at rest. During runtime, data can be decrypted within compute enclaves that isolate workloads from access initiating outside the enclave, enhancing runtime security and protecting data in-use.

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
- 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 3.2.1 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 3.2.1 and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

Calificación

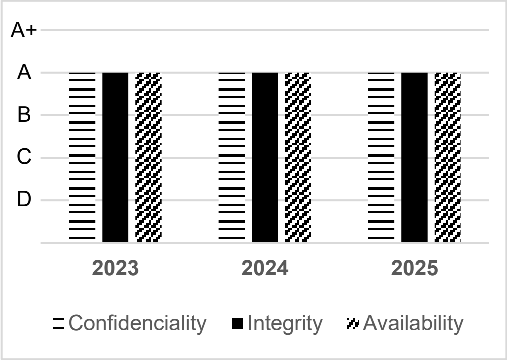
El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

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:

Cliente/Servicio – *Client/Service*: **ES0071/S002**
Referencia - *Reference*: **ES007100203582133**
Fecha de validez – *Valid until*: **Nov/29/2026**

A+	A+	A+
--A--	--A--	--A--
B	B	B
C	C	C
D	D	D
Confidencialidad *Confidentiality*	**Integridad** *Integrity*	**Disponibilidad** *Availability*



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

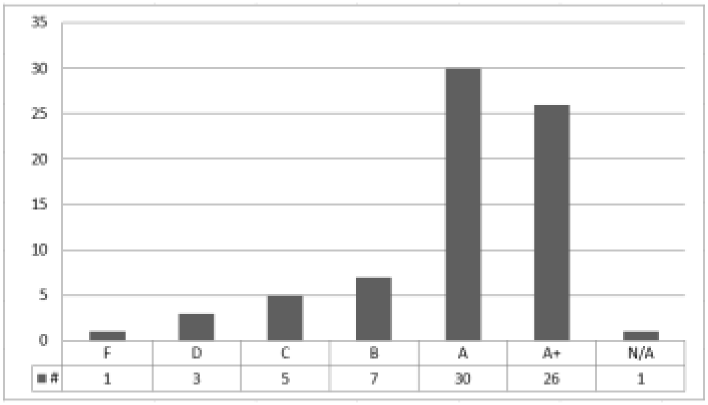
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad ‘1’.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad ‘2’.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad ‘3’.

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).

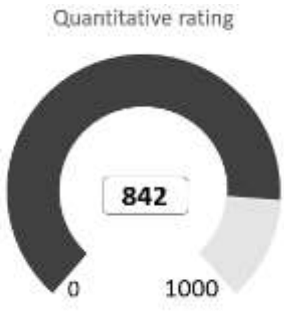
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- *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).



	F	D	C	B	A	A+	N/A
■ #	1	3	5	7	30	26	1



Madrid, November 11th, 2025

LEET SECURITY
CyberSecurity
Rating Agency

Firmado digitalmente por COLADO NUEVO, OSCAR (FIRMA)

Mr. Óscar Colado

Rating Evaluation Team – Operations Direction

Chief Auditor: Patricia López

LEET SECURITY
CyberSecurity
Rating Agency

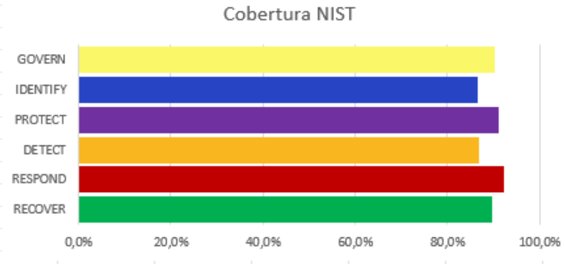
Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)

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].



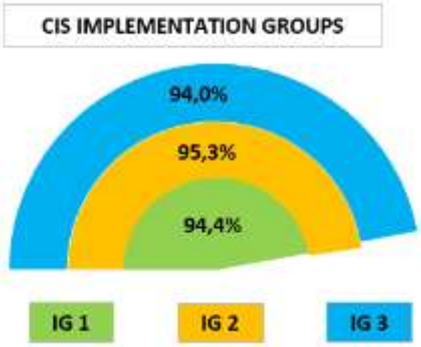
NIST coverage

This chart shows the implementation porcentaje of practices aplicable in the service, for the goal level reviewed (discolored bar) and for the máximum 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 7[2] están divididos en tres grupos: *Basic, Foundational y Organizational*, que a su vez de 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

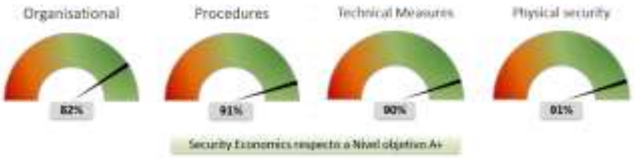
INFORMACIÓN ANALÍTICA DE SU EVALUACIÓN
ANALYTIC INFORMATION OF YOUR RATING

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.


Organisational
Procedures
Technical Measures
Physical security
Security Economics respecto a Nivel objetivo A+