



CyberSecurity
Rating Agency

Nivel de garantía
Level of assurance



Certified in EU

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0216/S001
Referencia - Reference: ES021600102453573
Fecha de validez – Valid until: 23 de mayo de 2023

Proveedor de servicio / Service provider

KYNDRYL España, S.A.

Identificación del servicio calificado / Rated Service identification

Servicios de externalización de infraestructuras
Infrastructure outsourcing services

Descripción del servicio calificado / Rated service description

Planificación, diseño, implementación, entrega y gestión de los servicios de externalización de infraestructura, que incluyen operaciones de sistemas de servidores, servicios de usuario final, gestión de servicios, servicios de red, seguridad y gestión de riesgos, gestión de activos, gestión de contratos, y la cuenta interna de Kyndryl, considerando:

- • Physical Security (Security):
 - Physical Security non-Kyndryl Datacenters and
 - Physical Security for Kyndryl Datacenters
- Archive Data Management (ADM) (Gestión de medios magnéticos)
- Security Management (R&C): Risk and Compliance.
 - Global SUDO Software and Template Management
 - Global Malware Defense Management/Antivirus
 - Global Password Strength
 - Global Firewall Rules Revalidation
 - Global Vulnerability Scanning
 - Global Technical Specification Life cycle Management
 - Global Privilege Monitoring
 - Global Principle of Least Privilege
 - Global Security Health Check
 - Global Cryptographic Key Management
 - Global Image Life Cycle Management
- Security Patch Management (Systems)
- Integrated Service Management (ISM)
 - Change Management
 - Incident Management
 - Problem Management
- Configuration Management / Security Inventory Management (ISM)
- Integrated Service Management (ISM)
- Disaster Recovery (Resiliency)
- Backup and Restore (Resiliency)
- IT Risk Management Services (R&C):
 - IT Risk Management
 - Issue Management
 - Security Policy Management
 - Exception Management
- Identity & Access Management (IAM)
 - ID Primary Controls
 - ID secondary Controls
- Configuration Item Build & Decommission:
 - Configuration Item Build & Decommission (high-level)
 - Server Build & Decommission
 - Mainframe Build & Decommission
 - Storage Build & Decommission
 - Network Build & Decommission

Planning, design, implementation, delivery and management of infrastructure outsourcing services, which include server system operations, end-user services, service management, network services, security and risk management, asset management, contract management, and Kyndryl's internal risk management, asset management, contract management, and Kyndryl's internal account, considering:

- *Physical Security (Security):*
 - *Physical Security non-Kyndryl Datacenters and*

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0216/S001
Referencia - *Reference*: ES021600102453573
Fecha de validez – *Valid until*: 23 de mayo de 2023

- *Physical Security for Kyndryl Datacenters*
- *Archive Data Management (ADM) (Gestión de medios magnéticos)*
- *Security Management (R&C): Risk and Compliance.*
 - *Global SUDO Software and Template Management*
 - *Global Malware Defense Management/Antivirus*
 - *Global Password Strength*
 - *Global Firewall Rules Revalidation*
 - *Global Vulnerability Scanning*
 - *Global Technical Specification Life cycle Management*
 - *Global Privilege Monitoring*
 - *Global Principle of Least Privilege*
 - *Global Security Health Check*
 - *Global Cryptographic Key Management*
 - *Global Image Life Cycle Management*
- *Security Patch Management (Systems)*
- *Integrated Service Management (ISM)*
 - *Change Management*
 - *Incident Management*
 - *Problem Management*
- *Configuration Management / Security Inventory Management (ISM)*
- *Integrated Service Management (ISM)*
- *Disaster Recovery (Resiliency)*
- *Backup and Restore (Resiliency)*
- *IT Risk Management Services (R&C):*
 - *IT Risk Management*
 - *Issue Management*
 - *Security Policy Management*
 - *Exception Management*
- *Identity & Access Management (IAM)*
 - *ID Primary Controls*
 - *ID secondary Controls*
- *Configuration Item Build & Decommission:*
 - *Configuration Item Build & Decommission (high-level)*
 - *Server Build & Decommission*
 - *Mainframe Build & Decommission*
 - *Storage Build & Decommission*
 - *Network Build & Decommission*

Alcance / *Scope*

Service offered with KYNDRYL's own equipment from KYNDRYL's or the client's facilities. Systems for the support and operation of all the DPCs providing the same service.

- Barcelona: Two DPCs, one office.

- Madrid: Two data centres, one office

For the management of its infrastructure outsourcing services, which include server system operations, end-user services, service management, network services, security and risk management, asset management, contract management, SOC managed security services, CMOS Cloud Services (On-Premises, Off-Premises or Hibryd) and Kyndryl's internal account.

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

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0216/S001
Referencia - Reference: ES021600102453573
Fecha de validez – Valid until: 23 de mayo de 2023

- 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 3.0 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 proces

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

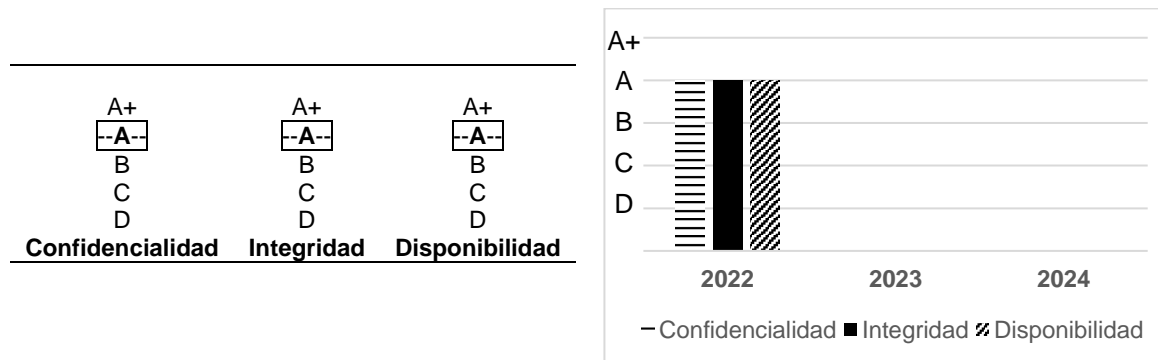
This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in rating methodology version 3.0 and evidences provided 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:



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

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0216/S001
Referencia - Reference: ES021600102453573
Fecha de validez – Valid until: 23 de mayo de 2023

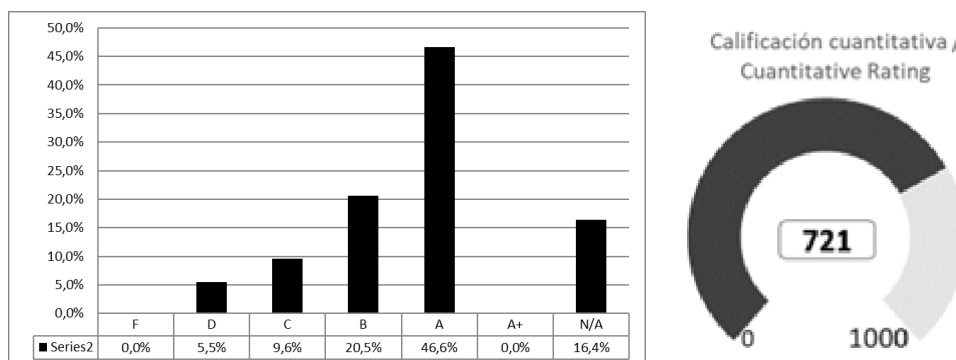
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad ‘1’.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad ‘2’.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad ‘3’.

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).



Madrid, 23 de julio de 2022 / July, 23th 2022

D. Rogelio Saavedra Collado
Rating Evaluation Team – Operations Direction