



CyberSecurity
Rating Agency

Nivel de garantía
Level of assurance



Certified in EU

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0040/S009
Referencia - *Reference*: ES004000901548892
Fecha de validez – *Valid until*: 31/12/2025

Proveedor de servicio / *Service provider*

RedSys Servicios de Procesamiento SL

Identificación del servicio calificado/

Rated Service identification

HUB OPEN BANKING

Descripción del servicio calificado /

Rated service description

La solución de HUB Open Banking está dirigida a las Entidades Financieras sujetas a la Directiva PSD2 de 2018 en el Acceso a Cuentas, por la que se obliga a las Entidades a dar acceso a terceros (Third Party Providers ó TPP) a las cuentas de pago de sus clientes, lo que permite a dichos terceros ofrecer servicios a través de la infraestructura de las Entidades.

Las Entidades financieras (APSP) están obligadas a desarrollar y publicar los interfaces que den acceso a las cuentas de sus clientes, y facilitar dicho acceso a todo tercero (TPP) que esté autorizado por el cliente, en las mismas condiciones en las que accede el cliente directamente, y sin necesidad de contrato entre el banco y el TPP, por lo que no se podrá cobrar a éste por el acceso.

El servicio de HUB Open Banking de Redsys facilita la conexión de los Proveedores de Servicios (TPP) a través de un único punto de acceso a las API de las entidades. Tiene un interfaz estándar para las comunicaciones que cubre los tres principales casos de uso: iniciación de pago, información de cuentas y confirmación de saldo.

Además de permitir la conexión, el HUB Open Banking ofrece otros servicios adicionales que permiten a las Entidades:

- Gestionar el control/monitorización/seguridad ante los nuevos requerimientos de PSD2
- Ahorro de costes y minimizan el impacto de la normativa.
- Simplicidad de aplicación de la normativa ya que para la gestión de ese acceso a terceros solo tendrá un interlocutor (Redsys) en lugar de tener que gestionar cada acceso con cada una de las empresas que se lo soliciten.
- Con la evolución de los volúmenes de servicio, incremento del valor de la información y del control y seguridad a Entidades.

The HUB Open Banking solution is aimed at Financial Institutions subject to the PSD2 Directive of 2018 on Account Access, which obliges the Institutions to give access to third parties (Third Party Providers or TPP) to the payment accounts of their customers, allowing such third parties to offer services through the infrastructure of the Institutions.

Financial Institutions (APSPs) are obliged to develop and publish the interfaces that give access to their customers' accounts, and provide such access to any third party provider (TPP) that is authorized by the customer, under the same conditions in which the customer accesses directly, and without the need for a contract between the bank and the TPP, so that the TPP cannot be charged for the access.

The Redsys Open Banking HUB service facilitates the connection of Service Providers (TPPs) through a single point of access to the institutions' APIs. It has a standard interface for communications covering the three main use cases: payment initiation, account information and balance confirmation.

In addition to enabling the connection, the Open Banking HUB offers other additional services that allow the Entities:

- *Manage control/monitoring/security in the face of the new PSD2 requirements.*
- *Cost savings and minimize the impact of the regulation.*
- *Simplicity in the application of the regulation, since for the management of this access to third parties there will only be one interlocutor (Redsys) instead of having to manage each access with each of the companies that request it.*
- *With the evolution of service volumes, increase in the value of the information and the control and security of the Entities.*

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0040/S009
Referencia - *Reference*: ES004000901548892
Fecha de validez – *Valid until*: 31/12/2025

Alcance / *Scope*

HUB central que facilita la conexión a los TPP, generando retorno a la industria bancaria.

Adicionalmente contiene un módulo de seguridad que cubre todos los requerimientos de seguridad que requerirán los nuevos servicios y protocolos. El módulo de entrada gestiona las llamadas con los TPP y el módulo de salida gestiona las llamadas con el banco. Se garantiza el acceso correcto de los TPP comprobando la fecha de validez de sus certificados y gestionando su propio certificado.

El servicio de HUB Open Banking cuenta con un módulo de monitorización que gestiona todas las peticiones recibidas, monitorizando de forma integral el sistema y permitiendo la definición de alertas.

Central HUB that facilitates the connection to the TPPs, generating return to the banking industry.

Additionally, it contains a security module that covers all the security requirements that the new services and protocols will require. The inbound module manages the calls with the TPPs and the outbound module manages the calls with the bank. The correct access of the TPPs is guaranteed by checking the validity date of their certificates and managing their own certificate. The HUB Open Banking service has a monitoring module that manages all incoming requests, monitoring the system comprehensively and allowing the definition of alerts.

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 3.1 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*

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0040/S009
Referencia - Reference: ES004000901548892
Fecha de validez – Valid until: 31/12/2025

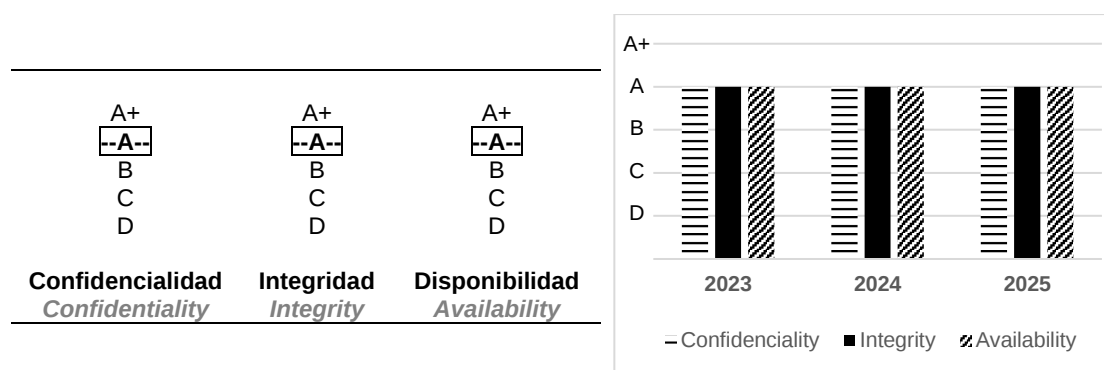
This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in rating methodology version 3.1 and evidences provided 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:



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).

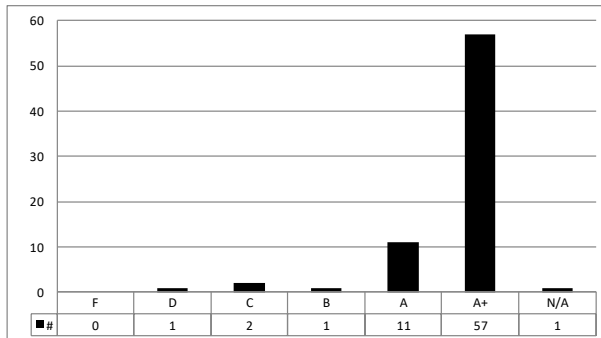
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- 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'.

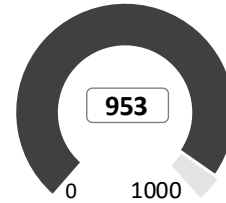
The evaluation of individual sections considers 100% of the controls (regardless of their priority) and it is showed in the following diagram. Quantitative rating is a weighted sum (base thousand) of levels achieved by sections (with a higher weight of those with a closer relation to agile security).

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0040/S009
Referencia - Reference: ES004000901548892
Fecha de validez – Valid until: 31/12/2025



Calificación cuantitativa /
Quantitative rating



Madrid, 14 de mayo de 2025/ May 14th, 2025

D. Patricia López Casado
Rating Evaluation Team – Operations Direction

Cliente/Servicio – *Client/Service*: ES0040/S009
Referencia - *Reference*: ES004000901548892
Fecha de validez – *Valid until*: 31/12/2025

ANEXO / ANNEX

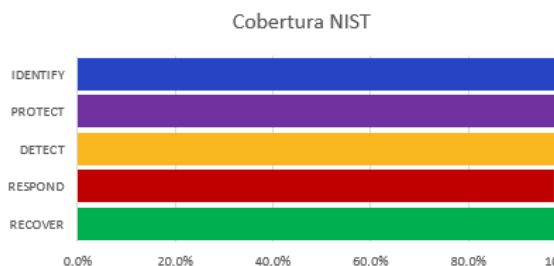
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES *INTERNATIONAL STANDARDS COVERAGE*

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

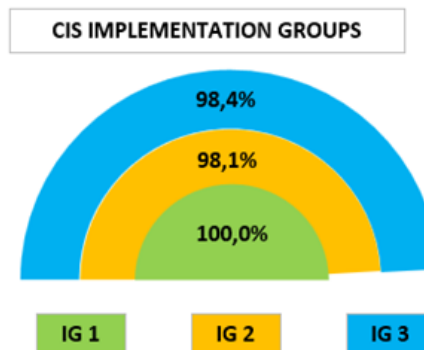
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

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>

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0040/S009
Referencia - *Reference*: ES004000901548892
Fecha de validez – *Valid until*: 31/12/2025

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.

