Cliente/Servicio – *Client/Service*: **ES0040/S003**
Referencia - *Reference*: **ES004000306475717**
Fecha de validez – *Valid until*: **31/12/2023**

Proveedor de servicio / *Service provider*

RedSys Servicios de Procesamiento, SL

Identificación del servicio calificado/ *Rated Service identification*

Adquirencia financiera/
Financial acquiring

Descripción del servicio calificado / *Rated service description*

Los servicios de adquirencia financiera ofrecen la oportunidad de conectar directamente los centros de demanda al nodo central de Redsys.

- Servicio de Cajeros: ofrece la posibilidad de tramitar y monitorizar las operaciones a las Entidades cuyos cajeros están conectados directamente a Redsys.
- Servicio de TPVs y de Grandes Establecimientos (GGEE): ofrece a los pequeños y grandes establecimientos la posibilidad de conexión a Redsys a través de un terminal punto de venta físico (TPV), para la gestión de operaciones principalmente de compra.
- Servicio TPV-PC: sistema web de compra presencial que permite a los comercios realizar operaciones con tarjeta, haciendo uso de un PC con PIN-Pad EMV, impresora y acceso a internet.
- Servicio mPOS: solución que permite convertir un dispositivo móvil (Smartphone o Tablet) en un terminal seguro de pago, mediante el uso de un PIN-Pad EMV y una aplicación móvil o Api integrable.
- Servicio de Comercio Electrónico (TPV Virtual): solución para las entidades que desean ofrecer a sus comercios una pasarela de pago en sus correspondientes sitios web. La plataforma ofrece todas las modalidades de pago existentes y cumple con las especificaciones de las marcas de tarjeta.

Financial acquiring services offer the opportunity to directly connect demand centers to the Redsys central node.

- *ATM Service: offers the possibility of processing and monitoring operations to Entities whose ATMs are directly connected to Redsys.*
- *POS and Large Establishments Service (GGEE): offers small and large establishments the possibility of connecting to Redsys through a physical point of sale terminal (POS), to manage mainly purchase operations.*
- *POS-PC service: web-based purchasing system that allows merchants to carry out card operations, using a PC with EMV PIN-Pad, printer and internet access.*
- *mPOS service: solution that allows converting a mobile device (Smartphone or Tablet) into a secure payment terminal, through the use of an EMV PIN-Pad and a mobile application or integrable API.*
- *Electronic Commerce Service (Virtual POS): solution for entities that wish to offer their businesses a payment gateway on their corresponding websites. The platform offers all existing payment methods and complies with the specifications of the card brands.*

Alcance / *Scope*

Los servicios de cajeros, TPV y grandes establecimientos están compuestos por pasarelas de comunicaciones (sobre sistemas distribuidos), que reciben las transacciones, y por los elementos de red (firewalls, balanceadores, VPN, routers, switches) a través de los cuales llegan a los sistemas transaccionales para su autorización.
Los servicios de comercio electrónico, TPVPC y mPOS están formados por las aplicaciones web SIS (TPV Virtual), TPVPC y Canales (administración de SIS y TPVPC) y los sistemas distribuidos (servidores web y de aplicación) y sistemas de información (base de datos) donde se ejecutan, junto a otros elementos de soporte (HSM y elementos de red como firewalls de red, firewalls de aplicación, balanceadores, routers, switches). Estos sistemas reciben transacciones provenientes de Internet y las transmiten a los sistemas transaccionales para su autorización.

Cliente/Servicio – *Client/Service*: **ES0040/S003**
Referencia - *Reference*: **ES004000306475717**
Fecha de validez – *Valid until*: **31/12/2023**

The services of ATMs, POS and large establishments are composed of communications gateways (on distributed systems), which receive transactions, and by network elements (firewalls, balancers, VPN, routers, switches) through which they reach transactional systems for authorization.
The electronic commerce services, TPVPC and mPOS are formed by the web applications SIS (Virtual POS), TPVPC and Channels (administration of SIS and TPVPC) and distributed systems (web and application servers) and information systems (database) where they run, along with other support elements (HSM and network elements such as network firewalls, application firewalls, balancers, routers, switches). These systems receive transactions from the Internet and transmit them to transactional systems for authorization.

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 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 3.1 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

Cliente/Servicio – ***Client/Service*****:** **ES0040/S003**
Referencia - ***Reference*****:** **ES004000306475717**
Fecha de validez – ***Valid until*****:** **31/12/2023**

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:

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

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

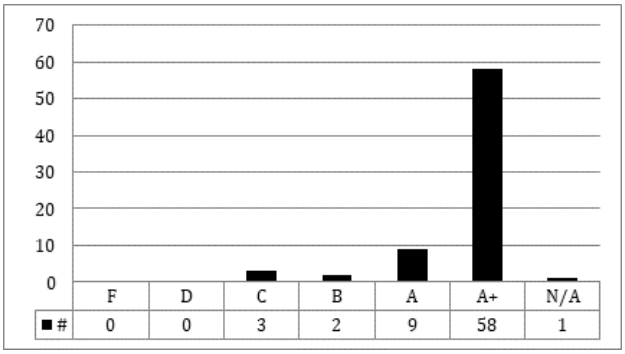
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

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).

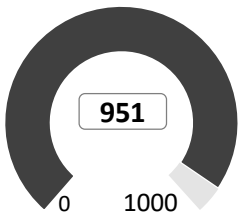
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- *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 /
Cuantitative rating



Madrid, 12 de mayo de 2023/ *May 12th, 2023*

Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)
Fecha: 2023.05.12 19:46:15 +02'00'

D. Patricia López Casado
Rating Evaluation Team – Operations Direction

Certifico la precisión e integridad de este documento

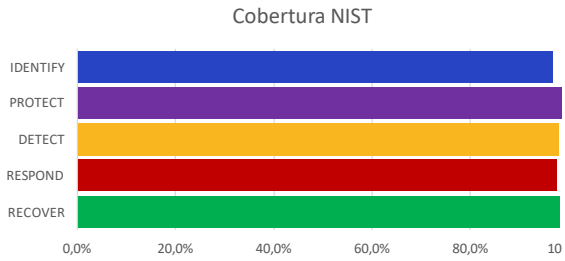
Cliente/Servicio – ***Client/Service*****:** **ES0040/S003**
Referencia - ***Reference*****:** **ES004000306475717**
Fecha de validez – ***Valid until*****:** **31/12/2023**

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].



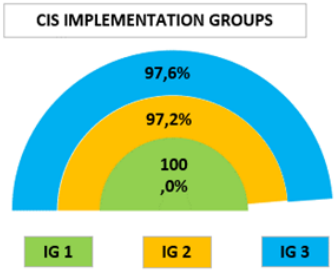
NIST coverage

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

Cliente/Servicio – ***Client/Service*****:** **ES0040/S003**
Referencia - ***Reference*****:** **ES004000306475717**
Fecha de validez – ***Valid until*****:** **31/12/2023**

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.