

Resumen ejecutivo de calificación / *Rating executive summary*
Pasaporte DORA / *DORA Passport*

Cliente/Servicio – *Client/Service*: ES0040/S008
Referencia - *Reference*: ES004000802585321
Fecha de validez – *Valid until*: 31/12/2026

Proveedor de servicio / *Service provider*

RedSys Servicios de Procesamiento SL

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

Servicios de Autenticación /
Authentication Services

**Descripción del
servicio calificado /
*Rated service
description***

El servicio de autenticación que implementa el componente ACS de EMV 3DSecure, es una solución de seguridad certificada por EMVCo, que se utiliza para verificar la identidad del titular de la tarjeta en transacciones de comercio electrónico y garantiza la seguridad de los pagos. Opera como intermediario entre el emisor, el titular de la tarjeta y la red de la marca (Visa Secure, Mastercard Id Check...), validando la identidad del usuario a través de diversos factores (como biometría, OTP, etc.). Realiza comunicación con los emisores para la autenticación del titular en banca móvil. Adicionalmente, permite autenticación sin fricción basadas en riesgo (denominada frictionless o exención), además de soportar entornos móviles y aplicaciones nativas

The authentication service implemented by the ACS component of EMV 3DSecure, is a security solution certified by EMVCo, which is used to verify the identity of the cardholder in e-commerce transactions and ensures the security of payments.

It operates as an intermediary between the issuer, the cardholder and the brand's network (Visa Secure, Mastercard Id Check...), validating the user's identity through various factors (such as biometrics, OTP, etc.).

It communicates with issuers for cardholder authentication in mobile banking. Additionally, it allows frictionless authentication based on risk (called frictionless or exemption), in addition to supporting mobile environments and native applications.

Alcance / *Scope*

Recibe las peticiones de solicitud de autenticación desde el entorno del comercio a través del componente de EMV 3DSecure denominado Directory Server.

Evalúa el riesgo de la transacción mediante Lynx analizando datos de la misma: información del titular, ubicación, dispositivo, entre otras.

Autenticación del titular de la tarjeta con posibilidad de autenticación basada en riesgo (frictionless) o desafío (challenge).

Realiza comunicaciones con los distintos emisores a través del hub de emisión con el objetivo de realizar la autenticación en la banca móvil del titular de la tarjeta (OoB)

Capacidades de autenticación en respaldo si existiesen problemas de comunicación con el emisor utilizando métodos de autenticación basados en OTP siempre que se disponga del teléfono del titular de la tarjeta

Exenciones aplicables TRA y LV:

- Exenciones por Análisis de riesgo de la transacción (TRA):
 - Puede ser solicitada por el comercio o el emisor
 - Puede aceptar la exención si el nivel de riesgo percibido es bajo, evaluando mediante Lynx.
- Exenciones por bajo valor (LV)
 - Se aplica a operaciones inferiores o iguales a 30 euros y puede ser gestionada directamente por el ACS sin requerir autenticación reforzada siempre que no se hayan superado un determinado número de transacciones consecutivas exentas o el total acumulado de transacciones exentas no supere una cantidad determinada en euros.

Cliente/Servicio – Client/Service: ES0040/S008
Referencia - Reference: ES004000802585321
Fecha de validez – Valid until: 31/12/2026

*Receives authentication request requests from the merchant environment through the 3DSecure EMV component called Directory Server.
Assesses transaction risk through Lynx by analyzing transaction data: cardholder information, location, device, among others.*

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
- Se incluirá en el sello el literal “DORA-PRIME”, en caso de que el índice de ciberresiliencia se encuentre entre 500 y 750 puntos y “DORA-ELITE” si dicho índice supera los 750 puntos.

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 más actual 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.*
- *The stamp will include the letters "DORA-PRIME" if the cyber resilience index is between 500 and 750 points, and "DORA-ELITE" if the index exceeds 750 points.*

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 the most recent version of the rating methodology and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

Calificación

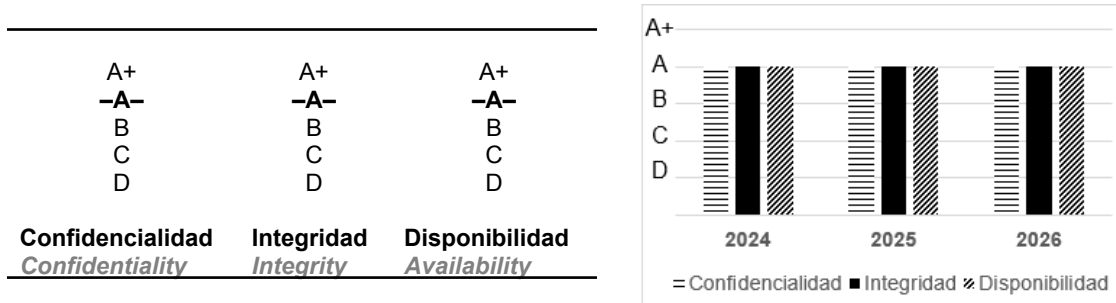
Resumen ejecutivo de calificación / Rating executive summary
Pasaporte DORA / DORA Passport

Cliente/Servicio – Client/Service: ES0040/S008
Referencia - Reference: ES004000802585321
Fecha de validez – Valid until: 31/12/2026

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:

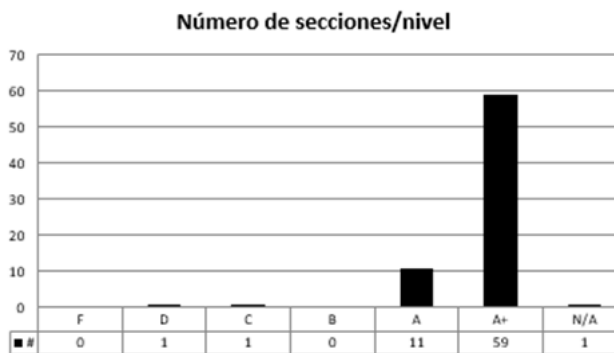
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

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).

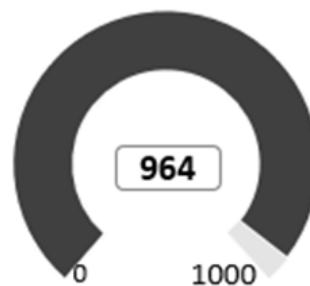
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- 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).



Calificación cuantitativa



Resumen ejecutivo de calificación / Rating executive summary
Pasaporte DORA / DORA Passport

Cliente/Servicio – Client/Service: ES0040/S008
Referencia - Reference: ES004000802585321
Fecha de validez – Valid until: 31/12/2026

Madrid, 25 de mayo de 2026/ 25th May 2026

D. Patricia Lopez
Rating Evaluation Team – Operations Direction

Cliente/Servicio – *Client/Service*: ES0040/S008
Referencia - *Reference*: ES004000802585321
Fecha de validez – *Valid until*: 31/12/2026

ANEXO I / ANNEX I

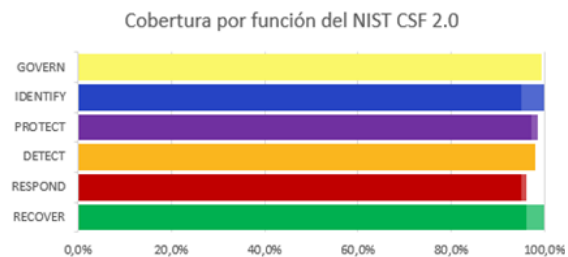
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES *INTERNATIONAL STANDARDS COVERAGE*

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 Cybersecurity Framework.



Cobertura respecto a CIS

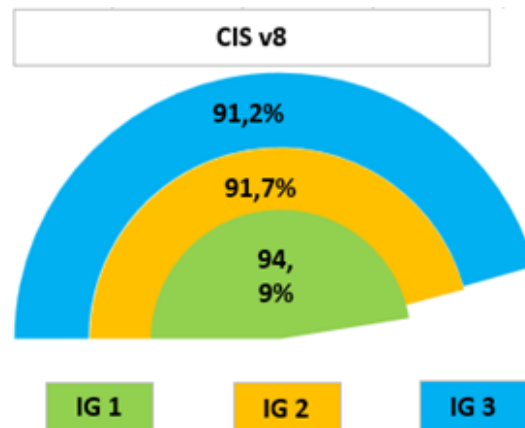
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 8² 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 8 are divided in three groups: Basic, Foundational and Organizational, that are also classified in three implementation 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/v8>

Cliente/Servicio – *Client/Service*: ES0040/S008
Referencia - *Reference*: ES004000802585321
Fecha de validez – *Valid until*: 31/12/2026

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.



ANEXO II pasaporte DORA *ANNEX II DORA passport*

Resultado de la evaluación final

El presente documento corresponde al informe adicional al propio de calificación de la tercera etapa del proceso de calificación y siempre debe utilizarse de manera conjunta. El "pasaporte DORA" 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 más actual y las evidencias aportadas por el mismo en la revisión documental u obtenidas por el equipo de la agencia durante la revisión in situ del proveedor del servicio.

Final assessment result

This document is a supplement to the assessment report for the third stage of the assessment process and should always be used in conjunction with it. The "DORA passport" is obtained on the basis of the responses provided by the service provider regarding the applicability and, where applicable, the existence of the controls included in the most recent version of the rating methodology, and the evidence provided by the service provider in the document review or obtained by the agency's team during the on-site review of the service provider.

Resumen ejecutivo

A continuación, se muestra el porcentaje de implantación en relación a los 5 pilares de DORA (RD 2024/1774):

Executive summary

The following table shows the percentage of implementation in relation to the five pillars of DORA (RD 2024/1774):

