Nivel de garantía
Level of assurance

Fully audited

Certified in EU

Resumen ejecutivo de calificación / ***Rating executive summary***

Cliente/Servicio – ***Client/Service*****:** **ES0040/S006**
Referencia - ***Reference*****:** **ES004000603512318**
Fecha de validez – ***Valid until*****:** **31/12/2024**

Proveedor de servicio / ***Service provider***

RedSys Servicios de Procesamiento, SL

Identificación del servicio calificado/
Rated Service identification

Bizum/
Bizum

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

Bizum es la solución de pagos a través del móvil, impulsada por la banca española, instantánea, rápida, cómoda y universal. Actualmente, permite realizar pagos entre particulares, donaciones a ONG y pagar en los comercios online asociados.
Bizum incluye un directorio de identidades que mediante la asociación móvil-IBAN permite desencadenar las órdenes de envío o solicitud de dinero entre particulares, sin necesidad de conocer el IBAN de destino. Este servicio incluye, además, el procesamiento de las órdenes para realizar la transferencia.
Tras la recepción de cualquier petición desde la entidad financiera cliente, Bizum verifica que los usuarios están dados de alta, asimismo, realiza verificaciones sobre los límites que aplican según Reglamento a la realización de pagos. Una vez realizadas y completas con éxito todas las validaciones lógicas y de negocio, se procede al envío de la orden de transferencia bancaria.
En la actualidad, Bizum ofrece dos servicios principales, incluyendo a su vez cada uno de ellos diversas funcionalidades:

- C2C pagos entre particulares (incluye entre otras funcionalidades C2ONG, que permite la realización de donativos a ONG).
- C2eR pago en comercio virtual.

Bizum is the instant, fast, convenient and universal mobile payment solution, promoted by Spanish banking. Currently, it allows you to make payments between individuals, donations to NGOs and pay at associated online stores.
Bizum includes a directory of identities that, through the mobile-IBAN association, allows sending orders or money requests to be triggered between individuals, without the need to know the destination IBAN. This service also includes the processing of orders to make the transfer.
After receiving any request from the client financial institution, Bizum verifies that the users are registered, likewise, it verifies the limits that apply according to the Regulations to making payments. Once all the logical and business validations have been carried out and successfully completed, the bank transfer order is sent. Currently, Bizum offers two main services, each of them including various functionalities:

- *C2C payments between individuals (including, among other functionalities, C2ONG, which allows donations to be made to NGOs).*
- *C2eR payment in virtual commerce.*

Alcance / ***Scope***

Conjunto de procesos (desarrollos internos), sistemas no transaccionales (Directorio)/ sistemas transaccionales donde éstos se ejecutan y módulos de seguridad (HSM), que permiten la recepción de transacciones provenientes de los entornos adquirentes y emisores.
Para algunas de estas transacciones también se incluirá el envío de la mismas para su autorización, bien por parte de los emisores o bien en Redsys (si la entidad lo ha delegado).

Set of processes (internal developments), non-transactional systems (Directory)/ transactional systems where they are executed and security modules (HSM), which allow the reception of transactions from the acquiring and issuing environments.
For some of these transactions, sending them for authorization will also be included, either by the issuers or by Redsys (if the entity has delegated it).

Cliente/Servicio – *Client/Service*: **ES0040/S006**
Referencia - *Reference*: **ES004000603512318**
Fecha de validez – *Valid until*: **31/12/2024**

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*

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:

Cliente/Servicio – ***Client/Service*****:** **ES0040/S006**
Referencia - ***Reference*****:** **ES004000603512318**
Fecha de validez – ***Valid until*****:** **31/12/2024**

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:

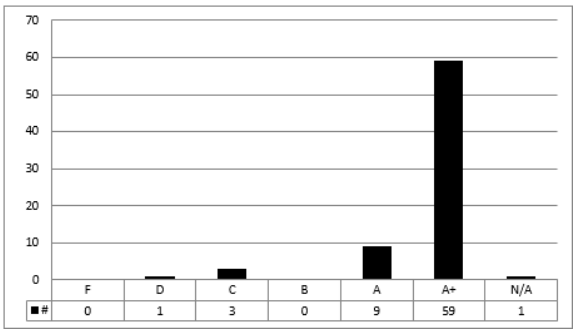
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

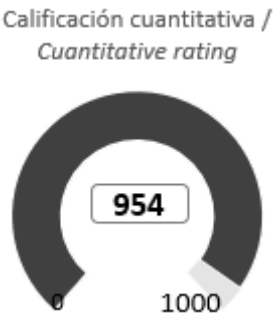
La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que 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).





Madrid, 17 de mayo de 2024/ *may 17, 2024*

Firmado digitalmente por COLADO NUEVO, OSCAR (AUTENTICACIÓN)
Fecha: 2024.05.20 16:57:13 +02'00'

D. Óscar Colado
Rating Evaluation Team – Operations Direction

Certifico la precisión e integridad de este documento

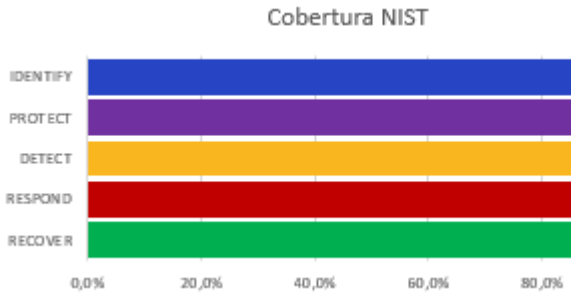
Cliente/Servicio – ***Client/Service*****:** **ES0040/S006**
Referencia - ***Reference*****:** **ES004000603512318**
Fecha de validez – ***Valid until*****:** **31/12/2024**

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].



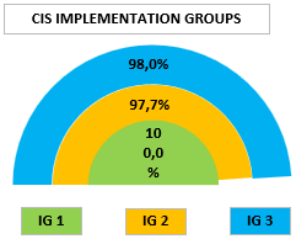
NIST coverage

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/S006**
Referencia - ***Reference*****:** **ES004000603512318**
Fecha de validez – ***Valid until*****:** **31/12/2024**

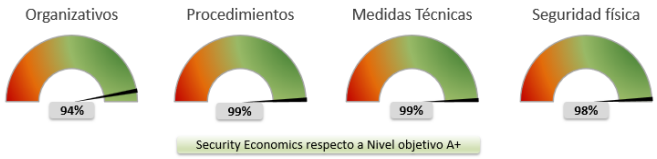
INFORMACIÓN ANALÍTICA DE SU EVALUACIÓN
ANALYTIC INFORMATION OF YOUR RATING

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.



Security Economics respecto a Nivel objetivo A+