

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0040/S004
Referencia - *Reference*: ES004000407512372
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*

Facturación de actos médicos/
Medical acts invoicing

Descripción del servicio calificado / *Rated service description*

Es el sistema de gestión de actos médicos que Chip Card ofrece a sus usuarios a través de la plataforma TVS (Termina Virtual Sanitario) y que además les permite a los profesionales médicos solicitar una autorización de servicios médicos utilizando un canal común entre todas las compañías aseguradoras de la Red. El sistema autoriza o deniega en función a las reglas de negocio definidas por las propias compañías sanitarias, que cargan en los sistemas. Diariamente éstas son informadas de toda la actividad que realiza su cartera de asegurados en su cuadro médico.

It is the medical event management system that Chip Card offers to its users through the TVS platform (Termina Virtual Sanitario) and that also allows medical professionals to request authorization for medical services using a common channel among all insurance companies network. The system authorizes or denies based on the business rules defined by the sanitation companies themselves, which are loaded into the systems. On a daily basis, they are informed of all the activity carried out by their insured portfolio in their medical directory.

Alcance / *Scope*

Aplicación TVS (Terminal Virtual Sanitario) y conjunto de sistemas distribuidos (servidores web y de aplicación), sistemas de información (base de datos), sistemas transaccionales y elementos de red (balanceadores, routers, switches, firewalls de red y de aplicación) que permiten la autorización de actos médicos.

TVS application (Virtual Sanitary Terminal) and set of distributed systems (web and application servers), information systems (database), transactional systems and network elements (balancers, routers, switches, network and application firewalls) that allow the authorization of medical acts.

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:

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0040/S004
Referencia - Reference: ES004000407512372
Fecha de validez – Valid until: 31/12/2024

- 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

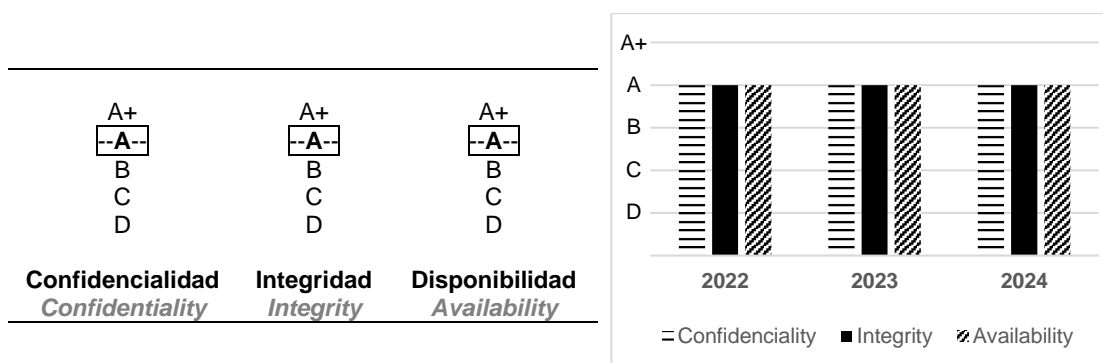
This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in rating methodology version 3.1 and evidences provided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



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'.



CyberSecurity
Rating Agency

Nivel de garantía
Level of assurance

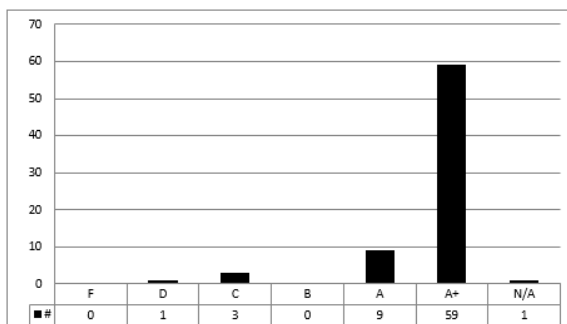


Certified in EU

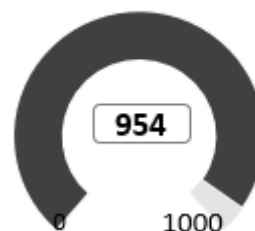
Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0040/S004
Referencia - Reference: ES004000407512372
Fecha de validez – Valid until: 31/12/2024

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 /
Quantitative rating



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

D. Óscar Colado
Rating Evaluation Team – Operations Direction

Cliente/Servicio – *Client/Service*: ES0040/S004
Referencia - *Reference*: ES004000407512372
Fecha de validez – *Valid until*: 31/12/2024

ANEXO / ANNEX

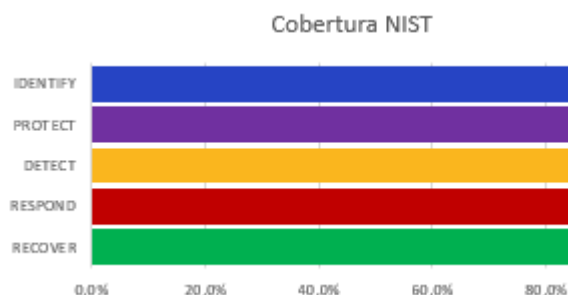
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES INTERNATIONAL STANDARDS COVERAGE

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 maximum level (intense bar) in each of the five steps of NIST Cybersecurity Framework.



Cobertura respecto a CIS

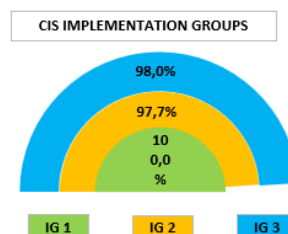
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 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/S004
Referencia - Reference: ES004000407512372
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.

