Cliente/Servicio – *Client/Service*: ES0002/S002
Referencia - *Reference*: ES000200211594678
Fecha de validez – *Valid until*: 3/04/2027

Proveedor de servicio / *Service provider*

Aiuken Solutions, S.L.

Identificación del servicio calificado/ *Rated Service identification*

Centro de Operaciones de Seguridad (SOC)/ *Security Operations Centre (SOC)*

Descripción del servicio calificado / *Rated service description*

El servicio SOC está compuesto por un conjunto de soluciones complementarias, modulares y escalables diseñadas para brindar a los clientes la capacidad de anticipar, detectar y responder a amenazas avanzadas, junto con soluciones robustas para mitigar los riesgos y una administración eficiente de sus clientes con vulnerabilidades TIC.

Este servicio se encargará de:

- Detectar y valorar, de modo periódico, las vulnerabilidades que presentan los equipos que integran la infraestructura tecnológica y los servicios publicados para poder abordar su adecuada mitigación.
- Proveer la capa de correlación en modo pago por uso.
- Configurar dicha capa para adaptarla a las necesidades del cliente integrando las diversas fuentes de eventos.
- Monitorizar las alertas de seguridad para detectar e investigar los incidentes de seguridad e informar de los mismos.
- Mitigar los incidentes de seguridad que puedan presentarse, bien por la detección de estos a través de los servicios ofertados o por su identificación por los profesionales del cliente.
- Informar de la posición de seguridad periódicamente a los responsables del cliente con objeto de facilitar la gestión de esta.

Los servicios serán prestados desde un Centro de Operaciones de Seguridad (SOC) externo al cliente y proporcionarán los instrumentos necesarios para gestionarlos de acuerdo con SLAs (Acuerdos de nivel de servicio) exigentes y medibles. Como resultado se proporciona al cliente los siguiente:

- Servicios gestionados de seguridad para cubrir las necesidades anteriormente identificadas en modo 24x7x365.
- Herramienta de ticketing (ITSM) integrada en el portal para poder realizar un seguimiento de alertas e incidentes.
- Informes mensuales de seguimiento del servicio.
- Informes de los incidentes de seguridad que sean gestionados.

The SOC service is composed of a set of complementary, modular and scalable solutions designed to provide customers with the ability to anticipate, detect and respond to advanced threats, along with robust risk mitigation solutions and efficient management of their customers' ICT vulnerabilities.

This service will be responsible for:

- *Detect and assess, on a regular basis, the vulnerabilities of the equipment that make up the technological infrastructure and the published services in order to be able to address their appropriate mitigation.*
- *Provide the correlation layer on a pay-per-use basis.Configure this layer to suit the customer's needs by integrating the various sources of events.*
- *Monitor security alerts to detect, investigate and report security incidents.*
- *Mitigate security incidents that may occur, either by detection through the services offered or by their identification by the client's professionals*
- *Report the security position on a regular basis to the customer's management in order to facilitate the management of the security position.*

The services will be provided from a Security Operations Centre (SOC) external to the customer and will provide the necessary tools to manage

them according to demanding and measurable SLAs (Service Level Agreements). As a result the customer is provided with the following:

- *Managed security services to cover the needs identified above in 24x7x265 mode.*
- *Integrated ticketing (ITSM) tool in the portal to track alerts and incidents.*
- *Monthly service monitoring reports.*
- *Reports of security incidents that are managed.*

Alcance / *Scope*

Los servicios del Centro de Operaciones de Seguridad (SOC) de Aiuken, se presta con equipamiento cloud y es gestionado por el personal de los SOC con los portátiles propios de la compañía.

Aiuken's Security Operations Centre (SOC) services are provided with cloud equipment and are managed by the SOC staff with the company's own laptops.

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 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.*

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

Cliente/Servicio – *Client/Service*: **ES0002/S002**
Referencia - *Reference*: **ES000200211594678**
Fecha de validez – *Valid until*: **3/04/2027**

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:

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:

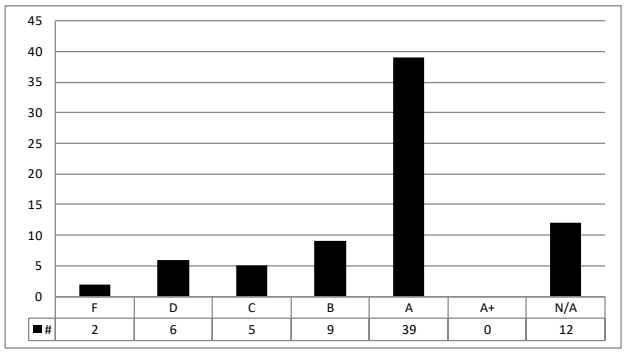
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

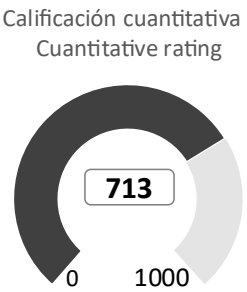
La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que 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, 30 de junio de 2026/ *June 30th, 2026*

Cliente/Servicio – *Client/Service*: **ES0002/S002**
Referencia - *Reference*: **ES000200211594678**
Fecha de validez – *Valid until*: **3/04/2027**

Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)

D. Patricia López
Rating Evaluation Team – Operations Direction

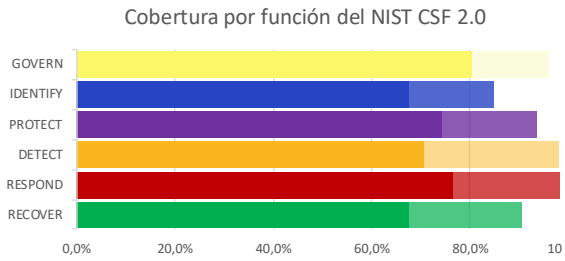
Cliente/Servicio – *Client/Service*: ES0002/S002
Referencia - *Reference*: ES000200211594678
Fecha de validez – *Valid until*: 3/04/2027

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].



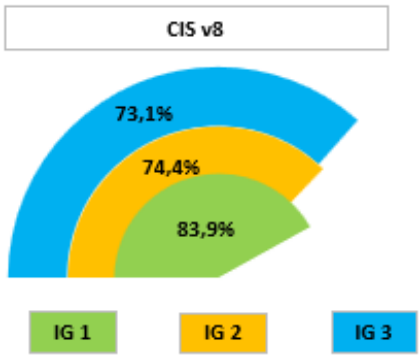
NIST coverage

This chart shows the implementation porcentaje of practices 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 8[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/v8

Cliente/Servicio – *Client/Service*: **ES0002/S002**
Referencia - *Reference*: **ES000200211594678**
Fecha de validez – *Valid until*: **3/04/2027**

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.