



CyberSecurity
Rating Agency



Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0002/S003
Referencia - *Reference*: ES000200310558152
Fecha de validez – *Valid until*: 04/03/2025

Proveedor de servicio / *Service provider*

Aiuken Solutions, S.L.

Identificación del servicio calificado/ *Rated Service identification*

Seguridad (WAF) en cloud/
Security (WAF) in cloud

Descripción del servicio calificado / *Rated service description*

Aiuken protege las aplicaciones web y sitios web con un cortafuegos para aplicaciones web (WAF) de clase empresarial mejorado gracias a la protección contra bots avanzada y los servicios de detección de shell de puerta trasera.

Publicar aplicaciones, sitios web o servicios en Internet hace que las necesidades de protección cambien. No es posible proteger estas aplicaciones con las barreras perimetrales tradicionales.

El WAF es la principal línea de defensa frente a los ataques a aplicaciones web, incluidas las 10 principales amenazas de OWASP.

El objetivo del Servicio WAF es redirigir el tráfico del sitio web a través de la plataforma, utilizando una redirección de DNS. Una vez que el tráfico se envía a nuestro sistema, será analizado por nuestras soluciones para detectar cualquier tráfico malicioso, como ataques a aplicaciones web, inyección SQL y scripts entre sitios, así como bots maliciosos, hackers, raspadores, spammers, etc.

Incluye el bloqueo de ataques técnicos como inyección SQL, scripts entre sitios, inclusión de archivos remotos que explotan vulnerabilidades en sitios web; ataques de lógica de negocio como scraping de sitios y spam de comentarios; botnets y ataques DDoS; y prevenir los intentos de adquisición de cuentas en tiempo real, antes de que se puedan realizar transacciones fraudulentas.

El tráfico legítimo es acelerado por la red de entrega de contenido del sistema, que proporciona una carga más rápida de sitios web.

Aiuken protects web applications and websites with an enterprise-class Web Application Firewall (WAF) enhanced by advanced bot protection and backdoor shell detection services.

Publishing applications, websites or services on the Internet changes the protection needs. It is not possible to protect these applications with traditional perimeter barriers.

The WAF is the main line of defence against web application attacks, including the OWASP top 10 threats.

The purpose of the WAF Service is to redirect website traffic through the platform, using DNS redirection. Once the traffic is sent to our system, it will be analysed by our solutions to detect any malicious traffic, such as web application attacks, SQL injection and cross-site scripting, as well as malicious bots, hackers, scrapers, spammers, etc.

It includes blocking technical attacks such as SQL injection, cross-site scripting, remote file inclusion that exploit vulnerabilities in websites; business logic attacks such as site scraping and comment spamming; botnets and DDoS attacks; and preventing account takeover attempts in real time, before fraudulent transactions can take place.

Legitimate traffic is accelerated by the system's content delivery network, which provides faster loading of websites.

Alcance / *Scope*

El servicio WAF Aiuken, se presta con equipamiento cloud y es gestionado por el personal de los SOC con los portátiles propios de la compañía.

The WAF Aiuken service is provided with cloud equipment and is managed by SOC staff with the company's own laptops.



CyberSecurity
Rating Agency



Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0002/S003
Referencia - *Reference*: ES000200310558152
Fecha de validez – *Valid until*: 04/03/2025

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

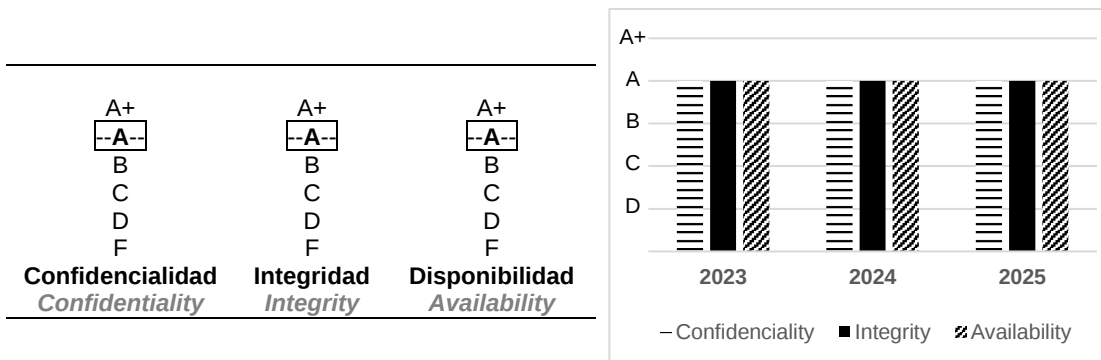
El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

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:

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0002/S003
Referencia - Reference: ES000200310558152
Fecha de validez – Valid until: 04/03/2025



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

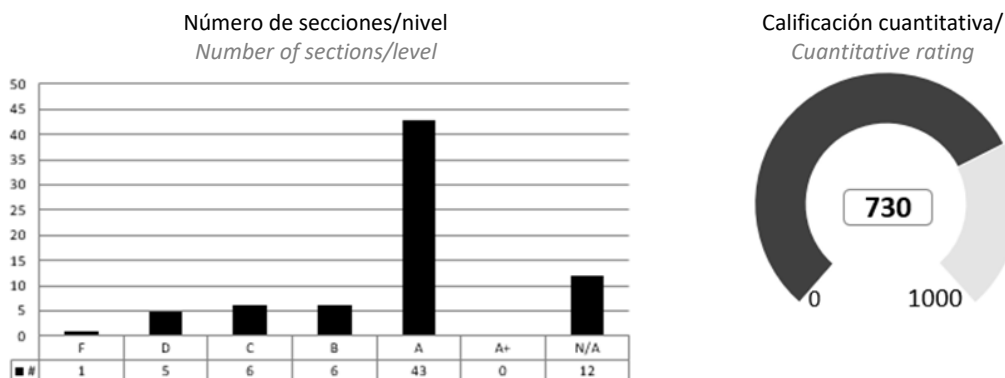
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

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, 13 de marzo de 2025 /March 13, 2025

D. Elena Miguel
Rating Evaluation Team – Operations Direction

Resumen ejecutivo de calificación / Rating executive summary

Cliente/Servicio – Client/Service: ES0002/S003
Referencia - Reference: ES000200310558152
Fecha de validez – Valid until: 04/03/2025

ANEXO / ANNEX

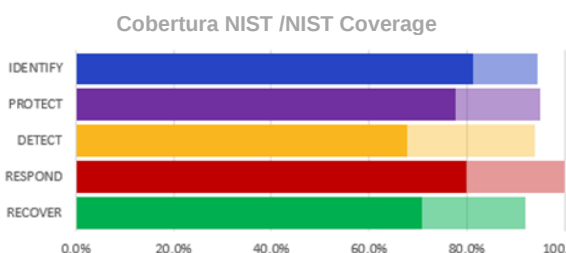
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES INTERNATIONAL STANDARDS COVERAGE

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 percentage 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

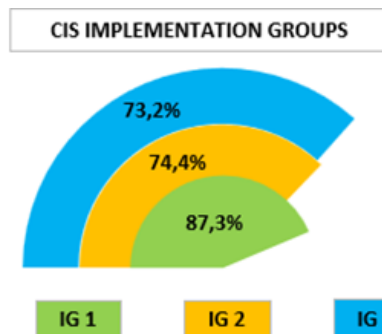
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 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>



CyberSecurity
Rating Agency



Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: ES0002/S003
Referencia - *Reference*: ES000200310558152
Fecha de validez – *Valid until*: 04/03/2025

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.

