Cliente/Servicio – *Client/Service* : **ES0002/S003**
Referencia - *Reference* : **ES000200307448526**
Fecha de validez- *Valid until* : **03 de abril de 2023**

Proveedor de servicio calificado ***Service provider***	**Identificación del servicio calificado** ***Rated Service identification***
Aiuken Solutions, S.L.	Centro de Operaciones de Seguridad (SOC) ***Security Operations Center (SOC)***

Descripción del servicio calificado

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 24x7x265.
- 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.

Rated service description

The SOC service consists 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:
- Detect and assess, on a regular basis, the vulnerabilities presented by 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 in pay-per-use mode.
- Configure this layer to adapt it to 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 identification by the customer's professionals.
- Periodically inform the client's managers of the security position in order to facilitate its management.

Cliente/Servicio – *Client/Service* : **ES0002/S003**
Referencia - *Reference* : **ES000200307448526**
Fecha de validez- *Valid until* : **03 de abril de 2023**

	The services will be provided from a Security Operations Centre (SOC) external to the customer and will provide the necessary tools to manage them in accordance with demanding and measurable SLAs (Service Level Agreements). As a result, the customer is provided with the following: ***- Managed security services to cover the above identified needs in 24x7x265 mode.*** ***- Integrated ticketing tool (ITSM) in the portal to track alerts and incidents.*** ***- Monthly service monitoring reports.*** ***- Reports of the security incidents that are managed.***
Alcance	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.
Scope	*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 3.0 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 proces

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 3.0 and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

Calificación

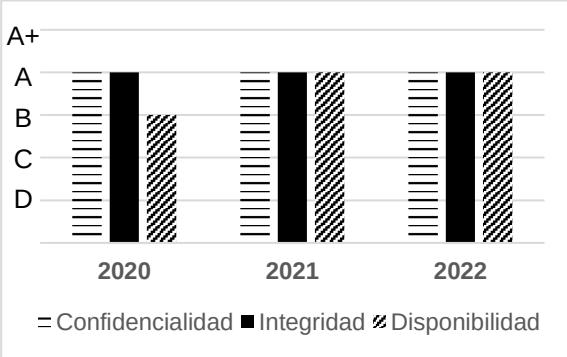
Cliente/Servicio – *Client/Service* : **ES0002/S003**
Referencia - *Reference* : **ES000200307448526**
Fecha de validez- *Valid until* : **03 de abril de 2023**

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:

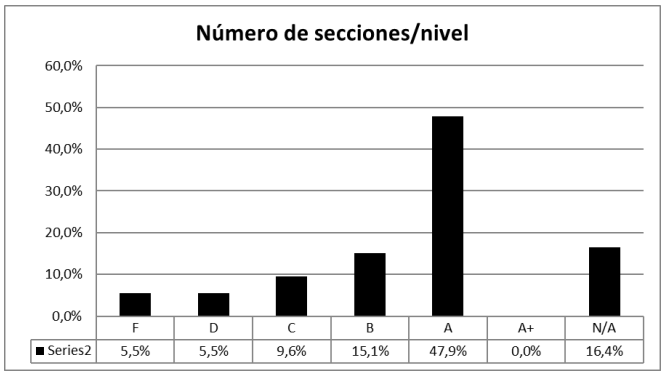
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad).

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. Cuantitative 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).



Cliente/Servicio – *Client/Service* **:** **ES0002/S003**
Referencia - *Reference* **:** **ES000200307448526**
Fecha de validez- *Valid until* **:** **03 de abril de 2023**

Madrid, 24 de marzo de 2022 / March*, 24th, 2022*

Firmado digitalmente por Rogelio Saavedra
Fecha: 2022.03.25 00:53:10 +01'00'

D. Rogelio Saavedra
Rating Evaluation Team – Operations Direction

Certifico la precisión e integridad de este documento