LEET SECURITY
CyberSecurity
Rating Agency

Nivel de garantía
Level of assurance
Fully audited
Certified in EU

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

Cliente/Servicio – ***Client/Service*****:** **ES0166/S001**
Referencia - ***Reference*****:** **ES016600101470922**
Fecha de validez – ***Valid until*****:** **13/11/2023**

Proveedor de servicio / ***Service provider***	**Identificación del servicio calificado/** ***Rated Service identification***
Innotec Security	Servicios de consultoría (entre los que se incluye la seguridad ofensiva)/ *Consulting services (including offensive security)*

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

El alcance de **Innotec** para la calificación de Pinakes se refiere a las siguientes modalidades de negocio que Innotec ofrece a sus clientes:

- Servicios de **consultoría** (entre los que se incluye seguridad ofensiva) – Donde los profesionales de Innotec ofrecen a sus clientes un estudio minucioso del estado de ciberseguridad de sus empresas. Gracias a ello, les ayuda a dar cobertura a sus problemas, realizando estudios detallados, analizando todos los puntos de ciberseguridad de su negocio y enviando un informe de las debilidades y mejoras detectadas.

Innotec's scope for the Pinakes rating refers to the following business modalities that Innotec offers to its clients:

- *Consulting services - (Including offensive security) - Where Innotec professionals offer their clients a detailed study of the cybersecurity status of their companies.*
  Thanks to this, it helps them cover their problems, carrying out detailed studies, analyzing all the cybersecurity points of their business and sending a report on the weaknesses and improvements detected.

Alcance / ***Scope***

Innotec se encarga del desarrollo y ejecución de proyectos y servicios gestionados, orientados a ofrecer y mejorar la ciberseguridad protegiendo sistemas, redes y programas de ataques digitales. Entre los servicios que se prestan se encuentran:

- **Security Monitoring & MDR**: Monitorización 24 x 7 de eventos de seguridad detectados (IDS/IPS, SIEM, etc.) y de la información que fluye por internet en busca de cualquier evento que pueda afectar a la imagen de marca o reputación del cliente Detección y protección contra ataques de reputación o contra directivos.
- **Digital Forensics and Incident Response**: Equipo de respuesta ante incidentes. Detección, investigación y respuesta ante amenazas de ciberseguridad.
  Una de las partes de esta área es el análisis forense digital. Este recopila datos de los sistemas de información, los analiza y los reconstruye para usarlos como evidencia en el proceso de respuesta a incidentes.
- **Malware & Forensics**: Estudio sobre la funcionalidad, origen e impacto potencial de una muestra determinada de malware, para evitar el robo de datos confidenciales de usuarios, organizaciones y empresas.
- **Cibertheats and intelligence**: Recopila y analiza los datos relacionados con un ciberataque, amplia y comparte el conocimiento sobre ese incidente, consolidando la capacidad de detección y anticipación ante nuevos riesgos.
- **Infrastructure Security**: Departamento desde el que se gestiona la infraestructura TI, soporte a los servicios internos, así como el mantenimiento de la infraestructura específica de proyectos.

Por otra parte, Innotec proporciona asesoramiento estratégico en materia de seguridad y riesgos tecnológicos. Determina el nivel de detección y de capacidad de la organización para la protección frente a amenazas. Esto se realiza gracias a:

- **Offensive security**: Detección de riesgos y vulnerabilidades mediante análisis de la situación real de las redes, servicios, sistemas, aplicaciones o infraestructura del cliente. También se obtiene una visión del impacto y el alcance de una intrusión real utilizando todos los recursos que un atacante puede disponer.
- **Consulting**: Consultoría y auditoría del cumplimiento normativo y de estándares internacionales. Elaboración y prueba de planes de contingencia y de continuidad de negocio. Análisis de riesgos y elaboración de planes directores de seguridad.

Innotec is in charge of the development and execution of projects and managed services, aimed at offering and improving cybersecurity by protecting systems, networks and programs from digital attacks. Among the services provided are:

- *Security Monitoring & MDR: 24 x 7 monitoring of detected security events (IDS/IPS, SIEM, etc.) and of the information that flows over the Internet in search of any event that may affect the client's brand image or reputation. Detection and protection against attacks on reputation or against managers.*
- *Digital Forensics and Incident Response: Incident response team. Detection, investigation and response to cybersecurity threats.*
  One of the parts of this area is digital forensics. It collects data from information systems, analyzes it, and reconstructs it for use as evidence in the incident response process.
    - *Malware & Forensics: Study on the functionality, origin and potential impact of a specific sample of malware, to prevent the theft of confidential data from users, organizations and companies.*
- *Cyberheats and intelligence: Collects and analyzes data related to a cyberattack, expands and shares knowledge about that incident, consolidating the ability to detect and anticipate new risks.*
- *Infrastructure Security: Department from which the IT infrastructure is managed, support for internal services, as well as maintenance of the specific project infrastructure.*

On the other hand, Innotec provides strategic advice on security and technological risks. Determines the organization's level of detection and ability to protect against threats. This is done thanks to:

- *Offensive security: Detection of risks and vulnerabilities through analysis of the real situation of the client's networks, services, systems, applications or infrastructure. You also get a view of the impact and scope of a real intrusion using all the resources an attacker can command.*
- *Consulting: Consulting and auditing of regulatory compliance and international standards. Preparation and testing of contingency and business continuity plans. Risk analysis and development of security master plans.*

Cliente/Servicio – *Client/Service*: **ES0166/S001**
Referencia - *Reference*: **ES016600101470922**
Fecha de validez – *Valid until*: **13/11/2023**

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

Calificación

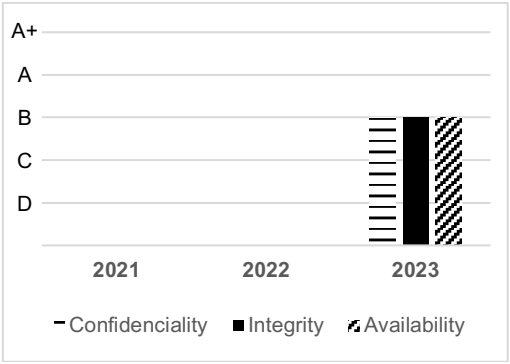
El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

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*: **ES0166/S001**
Referencia - *Reference*: **ES016600101470922**
Fecha de validez – *Valid until*: **13/11/2023**

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:

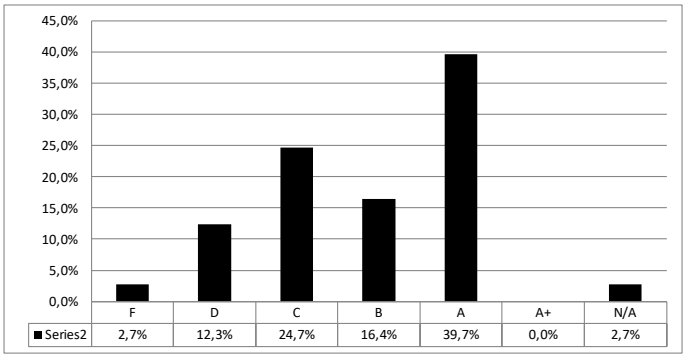
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

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, 14 de abril de 2023/ *April 14th, 2023*

Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)
Fecha: 2023.05.08 16:40:06 +02'00'

D. Patricia López Casado
Rating Evaluation Team – Operations Direction

Certifico la precisión e integridad de este documento

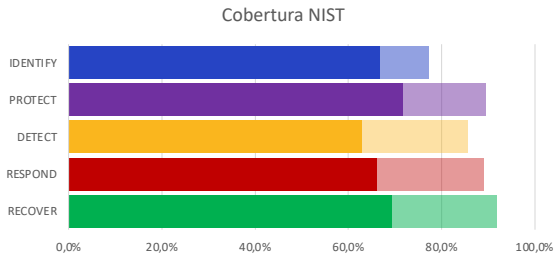
Cliente/Servicio – *Client/Service*: **ES0166/S001**
Referencia - *Reference*: **ES016600101470922**
Fecha de validez – *Valid until*: **13/11/2023**

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].



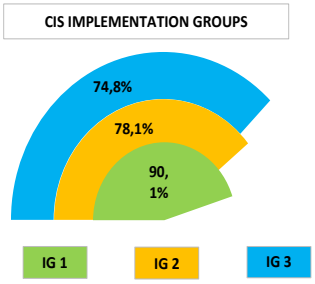
NIST coverage

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*****:** **ES0166/S001**
Referencia - ***Reference*****:** **ES016600101470922**
Fecha de validez – ***Valid until*****:** **13/11/2023**

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.