POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Alneux Sistemas Predictivos S.L.

Conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y a la Guía CCN-STIC-805

TABLA DE REVISIONES		
REVISIÓN	**FECHA**	**MOTIVO DE LA REVISIÓN**
01	01/10/2026	Emisión Inicial.

DOCUMENTO PREPARADO Y REVISADO		
FIRMA	**FECHA**	**PERSONA - CARGO**
Esteban Husillos	01/10/2026	Esteban Husillos **Resp. Sistemas**

APROBACIÓN DOCUMENTO		
FIRMA	**FECHA**	**PERSONA - CARGO**
Fernando Serrano	01/10/2026	Fernando Serrano **DIRECTOR**

El personal relacionado a continuación está autorizado para acceder al presente documento:

Responsable:	**Responsable SI.**
Lista de personal autorizado a acceder al documento:	Todo el personal de la Entidad.

1. Aprobación y Entrada en Vigor

El presente texto ha sido aprobado el día 1 de octubre de 2026 por Fernando Serrano, en su calidad de Director de Alneux Sistemas Predictivos S.L., en ejercicio de las máximas competencias ejecutivas de la organización.

Esta Política de Seguridad de la Información entra en vigor desde la fecha de aprobación y permanecerá vigente hasta que sea reemplazada por una nueva versión aprobada conforme al procedimiento establecido en la sección 12 del presente documento.

2. Introducción

Alneux Sistemas Predictivos S.L. (en adelante "Alneux") es una empresa tecnológica especializada en el desarrollo de sistemas de inteligencia artificial predictiva basados en tecnología propia denominada "Neurovectores". La organización ofrece soluciones de analítica avanzada a empresas e instituciones públicas, siendo proveedora de servicios tecnológicos a entidades de las Administraciones Públicas.

Alneux depende de los sistemas de información para alcanzar sus objetivos de negocio y prestar los servicios para los que ha sido constituida. Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad de la información tratada y los servicios prestados.

En virtud de su actividad como prestadora de servicios a entidades del sector público, Alneux queda sujeta al ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), de conformidad con su artículo 2. En consecuencia, la organización debe contar con una Política de Seguridad de la Información formalmente aprobada por el órgano competente.

Los sistemas TIC de Alneux deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

La seguridad TIC debe ser una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

3. Alcance

La presente Política de Seguridad de la Información se aplica a:

- Todos los sistemas de información de Alneux que dan soporte a los servicios prestados a entidades de las Administraciones Públicas y al sector privado, con especial atención a aquellos incluidos en el alcance de la certificación ENS.
- Todas las personas que forman parte de la organización: empleados, colaboradores, personal de dirección y cualquier persona que acceda a los sistemas de información de Alneux.
- Los prestadores de servicios y proveedores de soluciones TIC que, en virtud de una relación contractual, tengan acceso a los sistemas de información, activos o datos de Alneux.

El alcance detallado de los sistemas de información sujetos al ENS se describe en el documento ALX-ENS-00 "Alcance de Certificación ENS Categoría MEDIA".

4. Misión y Objetivos de Seguridad

4.1 Misión de la Organización

Alneux Sistemas Predictivos S.L. tiene como misión el desarrollo y la comercialización de soluciones de inteligencia artificial predictiva que permitan a las organizaciones mejorar sus procesos de toma de decisiones mediante el análisis avanzado de datos. Sus productos principales son la plataforma NEBOMIND para la automatización de procesos mediante agentes virtuales, y el Clasificador Predictivo basado en tecnología Neurovectores propia.

4.2 Objetivos de Seguridad

Los objetivos en materia de seguridad que Alneux pretende garantizar con la presente Política son:

- Garantizar la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de la información y la continuidad en la prestación de los servicios, conforme a las dimensiones de seguridad del ENS.
- Implementar medidas de seguridad proporcionadas al riesgo identificado, en cumplimiento del Esquema Nacional de Seguridad en Categoría MEDIA.
- Concienciar y formar a todos los integrantes de Alneux respecto a la seguridad de la información. Implementar medidas que permitan la trazabilidad de los accesos y respetar el principio de mínimo privilegio.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida, garantizando la seguridad por defecto.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando medidas para que los mismos no vuelvan a reproducirse.
- Proteger la información personal adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento, conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. Principios Rectores de la Política de Seguridad

La Política de Seguridad de la Información de Alneux se rige por los principios básicos establecidos en el Capítulo II del Real Decreto 311/2022 (artículos 5 a 11):

5.1 Seguridad integral (art. 6 ENS)

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

5.2 Gestión de la seguridad basada en los riesgos (art. 7 ENS)

La gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas, y serán proporcionales al riesgo que tratan. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

5.3 Prevención, detección, respuesta y conservación (art. 8 ENS)

Alneux implementará acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

5.4 Existencia de líneas de defensa (art. 9 ENS)

La estrategia de seguridad de Alneux se diseña e implementa en capas de seguridad, de modo que el compromiso de una sola no implique la vulneración de todo el sistema. Las líneas de defensa se establecen mediante controles complementarios que reducen el riesgo residual.

5.5 Vigilancia continua y reevaluación periódica (art. 10 ENS)

Alneux implementará medios para la detección y respuesta a actividades o comportamientos anómalos. Existirá un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

5.6 Diferenciación de responsabilidades (art. 11 ENS)

En aplicación de este principio, las funciones del Responsable de la Información, del Responsable del Servicio, del Responsable de la Seguridad y del Responsable de los Sistemas estarán diferenciadas, evitando incompatibilidades y conflictos de interés.

5.7 Seguridad por defecto y desde el diseño

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados. La seguridad se incorporará como requisito desde las fases iniciales del diseño y desarrollo de los sistemas.

6. Marco Normativo

Las principales normas que afectan a la presente Política de Seguridad de la Información son:

Norma / Referencia	Descripción
Real Decreto 311/2022, de 3 de mayo	Por el que se regula el Esquema Nacional de Seguridad. Marco normativo principal de referencia para la seguridad de los sistemas de información.
Ley 40/2015, de 1 de octubre	Régimen Jurídico del Sector Público. Establece la obligatoriedad del ENS para las AA.PP. y sus proveedores.
Ley 39/2015, de 1 de octubre	Procedimiento Administrativo Común de las Administraciones Públicas.
Reglamento (UE) 2016/679 — RGPD	Reglamento General de Protección de Datos. Regula el tratamiento de datos personales y la libre circulación de estos datos en la Unión Europea.
Ley Orgánica 3/2018 — LOPDGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

Directiva (UE) 2022/2555 — NIS2	Medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión Europea.
CCN-STIC-800 y series relacionadas	Guías del Centro Criptológico Nacional para la implantación y cumplimiento del ENS. En particular: CCN-STIC-801 (Responsables), CCN-STIC-802 (auditoría), CCN-STIC-803 (valoración), CCN-STIC-804 (medidas), CCN-STIC-805 (política), CCN-STIC-806 (plan adecuación).
ISO/IEC 27001:2022	Sistema de Gestión de la Seguridad de la Información (SGSI). Norma complementaria al ENS.
ISO/IEC 22301:2019	Sistema de Gestión de la Continuidad del Negocio (SGCN).

La normativa de seguridad interna de Alneux se desarrolla mediante normas, guías y procedimientos de seguridad que concretan las directrices de esta Política. Dicha normativa estará disponible para todos los miembros de la organización a través de los canales internos de comunicación habilitados al efecto.

7. Organización de la Seguridad

7.1 Comité de Seguridad de la Información

El Comité de Seguridad de la Información de Alneux es el órgano colegiado responsable de la dirección y supervisión de la seguridad de la información en la organización. Está constituido conforme al Acta de Constitución ALX-RSSI-01.1.

Composición: El Comité estará presidido por el Director (Fernando Serrano) y contará con la participación del Responsable de Sistemas (Esteban Husillos Bernal). Podrán incorporarse otros miembros o asesores externos cuando las circunstancias lo requieran.

Funciones principales: Aprobar y revisar la Política de Seguridad y la normativa de seguridad; supervisar el estado de seguridad de los sistemas; aprobar los planes de tratamiento de riesgos; resolver conflictos entre los responsables de seguridad; impulsar la mejora continua del sistema de gestión.

Reuniones: El Comité se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo requieran circunstancias excepcionales (incidentes graves, cambios normativos significativos, modificaciones sustanciales en los sistemas).

7.2 Roles de Seguridad (art. 11 RD 311/2022)

Conforme al artículo 11 del Real Decreto 311/2022, se establecen los siguientes roles de seguridad con sus atribuciones y mecanismos de coordinación:

Rol ENS	Titular	Principales Funciones y Responsabilidades
Responsable de la Información	Fernando Serrano	Determinar los requisitos de la información en materia de seguridad. Es el propietario de la información tratada en el sistema y establece los niveles de seguridad exigibles a cada activo de información.
Responsable del Servicio	Fernando Serrano	Determinar los requisitos del servicio en materia de seguridad. Define los niveles de disponibilidad y continuidad necesarios para el correcto funcionamiento de los servicios prestados.
Responsable de la Seguridad (RSSI)	Fernando Serrano	Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información. Elaborar y mantener la política de seguridad. Supervisar el cumplimiento de las medidas de seguridad. Gestionar incidentes de

		seguridad. Actuar como Punto de Contacto (POC) ante el CCN-CERT.
Responsable de los Sistemas (RSI)	Esteban Husillos Bernal	Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Implementar las medidas de seguridad acordes con los requisitos establecidos por el RSSI. Gestionar los cambios en los sistemas y garantizar su operación segura y continua.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por incumplimiento reiterado de sus funciones, previo apercibimiento. La organización dispondrá de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias.

7.3 Resolución de Conflictos

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias. Las decisiones del Comité serán de obligado cumplimiento para todos los responsables. Si el conflicto afectara a la integridad del sistema o a la continuidad del servicio, prevalecerá el criterio del Responsable de la Seguridad hasta que el Comité resuelva.

8. Directrices para la Estructuración de la Documentación de Seguridad

La documentación de seguridad de Alneux se estructura en los siguientes niveles, de mayor a menor nivel de abstracción:

Nivel	Tipo de Documento	Descripción
Nivel 1	Política de Seguridad	Documento de alto nivel que establece las directrices generales (el presente documento ALX-ENS-02).
Nivel 2	Normas de Seguridad	Establecen requisitos específicos sobre aspectos concretos (control de acceso, gestión de contraseñas, uso aceptable, etc.).
Nivel 3	Procedimientos de Seguridad	Describen paso a paso cómo llevar a cabo tareas específicas de seguridad (gestión de incidentes, copias de seguridad, auditorías, etc.).
Nivel 4	Guías y Registros	Documentos de apoyo, buenas prácticas, plantillas y evidencias del cumplimiento (registros de auditoría, informes de incidentes, actas, etc.).

La gestión documental se realizará conforme a los criterios de clasificación, control de versiones y acceso establecidos por el Comité de Seguridad de la Información. Toda la documentación de seguridad será accesible para las personas que necesiten conocerla en el ejercicio de sus funciones.

Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la Política de Seguridad de la Información en los aspectos que les afecten, conforme a lo establecido en la medida [op.acc.6.1] del Anexo II del RD 311/2022.

9. Tratamiento de Datos Personales

Alneux trata datos de carácter personal en el ejercicio de su actividad, según se describe en el Registro de Actividades del Tratamiento. La organización evaluará los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, y en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizarse, en su caso, una evaluación de impacto (EIPD/DPIA). La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad derivados de las obligaciones en materia de protección de datos.

La política de seguridad recogerá los criterios que en Alneux determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el Anexo I del RD 311/2022, conforme a la medida [mp.info.2.3].

10. Gestión de Riesgos

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el artículo 7 del ENS. El análisis de riesgos se revisará y aprobará anualmente, conforme al apartado 1.1 d) del Anexo III del ENS.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios en la información manejada.
- Cuando se produzcan cambios en los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

El Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Los responsables de los sistemas realizarán los análisis de riesgos atendiendo a sus conclusiones y gestionarán los riesgos por encima del umbral asumible acordado.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. Concienciación y Formación

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de Alneux y a todas las actividades, de acuerdo con el principio de Seguridad como proceso integral recogido en el artículo 6 del ENS.

Todos los miembros de Alneux tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen. Será responsabilidad de la organización, a través del Comité de Seguridad, disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Alneux atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación específica para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. Obligaciones del Personal

Todo el personal de Alneux, así como los colaboradores y terceros con acceso a los sistemas de información, tienen las siguientes obligaciones:

- Conocer y cumplir la presente Política de Seguridad de la Información y la normativa de seguridad que la desarrolle.
- Proteger la información a la que tienen acceso en el ejercicio de sus funciones, respetando el principio de confidencialidad y el deber de secreto profesional.
- Utilizar los sistemas de información únicamente para los fines autorizados y en la medida necesaria para el desempeño de sus funciones.
- Notificar de forma inmediata al Responsable de la Seguridad cualquier incidente de seguridad, brecha de seguridad o comportamiento anómalo que detecten en los sistemas.
- Participar en las actividades de formación y concienciación en materia de seguridad de la información organizadas por Alneux.
- Aplicar las medidas de seguridad establecidas en los procedimientos y normas de seguridad vigentes.
- No divulgar información confidencial a personas no autorizadas, tanto dentro como fuera de la organización.

El incumplimiento de las obligaciones establecidas en la presente Política y en la normativa de seguridad que la desarrolle podrá dar lugar a las responsabilidades establecidas en la legislación vigente y en los contratos laborales o de colaboración aplicables.

13. Terceras Partes, Prestadores de Servicios y Proveedores

Cuando Alneux preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios.

Cuando Alneux utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad que ataña a dichos servicios o información. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS. En la adquisición de derechos de uso de activos en la nube se tendrán en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II del RD 311/2022.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa aplicable, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Alneux podrá supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación.

El Responsable de la Seguridad (o persona en quien delegue) actuará como Punto de Contacto (POC) para la coordinación con terceros en materia de seguridad y para la gestión de incidentes que involucren a terceros.

14. Gestión de Incidentes de Seguridad

Alneux dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales (protección de datos, NIS2), y se establecerán canales para comunicar y coordinar los diferentes enfoques.

Se comunicará a las autoridades competentes sin dilaciones indebidas aquellos incidentes que así lo requieran. El Responsable de la Seguridad actuará como Punto de Contacto (POC) ante el CCN-CERT para la notificación y coordinación de incidentes significativos que afecten a los sistemas incluidos en el alcance ENS.

El procedimiento de gestión de incidentes contemplará, como mínimo:

- Identificación, clasificación y registro del incidente.
- Notificación inmediata al Responsable de la Seguridad.
- Análisis, contención y erradicación del incidente.
- Recuperación de los sistemas o servicios afectados.
- Análisis post-incidente y lecciones aprendidas.
- Notificación a las autoridades competentes cuando así lo exija la normativa (CCN-CERT, AEPD en caso de brecha de datos personales).

15. Desarrollo de la Política de Seguridad

Esta Política de Seguridad de la Información se complementa e integra junto con otras políticas de Alneux en diferentes materias. Se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de Alneux que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Entre los documentos de desarrollo previstos se encuentran, de manera no exhaustiva:

- Norma de uso aceptable de sistemas de información.
- Política de control de acceso y gestión de identidades.
- Política de gestión de contraseñas.
- Procedimiento de gestión de incidentes de seguridad.
- Procedimiento de análisis y gestión de riesgos.
- Procedimiento de auditoría y revisión de la seguridad.
- Plan de continuidad del servicio y recuperación ante desastres.
- Política de clasificación y manejo de la información.
- Norma de seguridad en el uso de servicios en la nube.
- Procedimiento de gestión de proveedores y terceros.

16. Aprobación, Revisión y Actualización de la Política

La presente Política de Seguridad de la Información ha sido aprobada formalmente por la Dirección de Alneux Sistemas Predictivos S.L. Estará sujeta a un proceso de revisión regular que la adapte a nuevas circunstancias técnicas u organizativas, y evite que quede obsoleta.

El proceso de revisión y actualización de la Política seguirá las siguientes pautas:

- El Comité de Seguridad de la Información revisará la Política con carácter ordinario al menos una vez al año.
- Las modificaciones que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información.
- En caso de que los cambios supongan una modificación sustancial de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados por la Dirección.
- La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la Dirección, informando adecuadamente a los interesados por los mismos canales usados para su difusión.
- Las actualizaciones motivadas exclusivamente por cambios normativos se tramitarán de manera simplificada, evitando la transcripción literal de artículos normativos en el cuerpo de la Política.

La Política será conocida por todas las personas que formen parte de Alneux e identificará de forma inequívoca a los responsables de velar por su cumplimiento, conforme a lo establecido en el artículo 13.2 del RD 311/2022.

Control de Versiones

Versión	Fecha	Descripción del Cambio	Autor
01	01/10/2026	Versión inicial de la Política de Seguridad de la Información de Alneux Sistemas Predictivos S.L., conforme al RD 311/2022 y la guía CCN-STIC-805.	Esteban Husillos Bernal

La presente POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ha sido aprobada por la DIRECCIÓN de ALNEUX SISTEMAS PREDICTIVOS, S.L., en fecha 01/10/2026.

Fernando Serrano

Fernando Serrano – DIRECCIÓN

En Málaga, a 01 de octubre 2026.