SISTEMA INTEGRADO DE GOBERNANZA (SIGG)

Plain Concepts, S.L.U. y sociedades del Grupo Plain Concepts

DOC-02

POLÍTICA Y MARCO DE DIRECCIÓN Y GOBERNANZA INTEGRADA

Documento normativo · Extensión: CORE · Capa del modelo: C2 · Núcleo de gobernanza (dirección y reglas del juego)

VERSIÓN 1.1	FECHA DE VERSIÓN 13/10/2026
ESTADO Aprobada	PRÓXIMA REVISIÓN 12 meses desde su aprobación
PROPIETARIO DEL DOCUMENTO Dirección de Sistema Integrado de Gestión (SIG) / Compliance · iso@plainconcepts.com	APROBADO POR Dirección
CLASIFICACIÓN Público · difusión general interna y externa	ÁMBITO DE APLICACIÓN Plain Concepts, S.L.U. y filiales; Ardanis Technologies Ltd. incluida en el alcance certificado
UBICACIÓN OFICIAL Handbook / Teams / OneDrive / SharePoint corporativo	CONSERVACIÓN Mientras esté vigente y 6 años tras su sustitución, salvo plazo legal superior

Control del documento

Historial de versiones

Versión	Fecha	Autor	Descripción del cambio	Aprobado por
Rev. 03	26/09/2023	Dirección	«Política del sistema integrado»: documento base vigente, con visión, misión, diez valores corporativos y compromiso de la Dirección. Publicado en la web corporativa.	Enrique Martínez Alén (Dirección)
2.0	31/07/2026	Dirección de SIG / Compliance	Revisión integral y ampliación de la Rev. 03: contexto organizativo, propiedad intelectual, transparencia y rendición de cuentas, gobernanza y responsabilidades, objetivos e indicadores, comunicación y formación, canal ético conforme a la Ley 2/2023 y reordenación del marco normativo.	Dirección
1.0 (SIGG)	07/09/2026	ISO controller	Incorporación de la Política Integrada v2.0 a la estructura del SIGG.	Dirección
1.1 (SIGG)	13/10/2026	Dirección de SIG	Integración completa del contenido de la Política Integrada Rev. 04 que no se había trasladado a la v1.0: contexto organizativo, alcance, valores, propiedad intelectual, transparencia, canal ético, roles, objetivos e indicadores, comunicación y marco normativo. Refuerzo de la declaración con los compromisos que exigen las normas. Propuesta de apetito de riesgo y de estructura de decisión. Eliminación de las instrucciones de la plantilla.	Dirección

Revisión y aprobación

Actuación	Rol / Órgano	Nombre	Fecha y firma
Elaborado por	ISO controller	Natalia Domínguez Peña	
Revisado por	Comité de Seguridad · Responsable de la Gestión de la Seguridad de la Información	Alejandro Casquete Prieto	
Aprobado por	Dirección · CEO	Enrique Martínez Alén	Véase el Anexo B

Relación con otros documentos del SIGG

Sentido	Documento / registro	Qué se toma o se entrega
Se apoya en	DOC-01	Alcance y normas integradas
Se apoya en	REG-04	Contexto y expectativas de las partes interesadas
Se apoya en	REG-03	Obligaciones que la política se compromete a cumplir
Alimenta a	REG-05	Marco de referencia para fijar objetivos
Alimenta a	DOC-04	Apetito y criterios de riesgo
Alimenta a	Todas las extensiones	Directrices específicas por materia
Se apoya en	REG-01	Órganos, delegaciones y responsabilidades nominales
Alimenta a	REG-08	Evidencias de comunicación y formación sobre la Política
Alimenta a	REG-10	Apetito de riesgo y quién acepta el riesgo residual
Alimenta a	REG-13	Incumplimientos de la Política y brechas pendientes

Índice

Control del documento **2**
Historial de versiones 2
Revisión y aprobación 2
Relación con otros documentos del SIGG 3
1. Declaración de la dirección **5**
Quiénes somos: contexto organizativo 5
Alcance y aplicación de la Política 6
2. Principios de gobernanza **6**
Propósito y valores corporativos 7
3. Directrices por materia **7**
Calidad y satisfacción del cliente 7
Medio ambiente 7
Cumplimiento y conducta 7
Seguridad de la información 8
Seguridad en el ámbito del ENS 8
Privacidad y protección de datos 8
Inteligencia artificial 8
Seguridad y salud en el trabajo 9
Continuidad de negocio 9
Propiedad intelectual e industrial 9
Transparencia y rendición de cuentas 9
4. Apetito de riesgo y criterios de tolerancia **10**
5. Estructura de decisión y delegación **10**
Roles y responsabilidades 11
6. Compromisos hacia las partes interesadas **12**
Objetivos estratégicos e indicadores de desempeño 12
7. Incumplimiento de la política **13**
Canal ético 13
8. Vigencia, difusión y revisión **14**
Anexo A. Trazabilidad normativa de este documento **15**
Anexo B. Firma y aprobación **17**

1. Declaración de la dirección

En Plain Concepts impulsamos la transformación digital de organizaciones de todo el mundo mediante la ingeniería de software, la inteligencia artificial, los datos, la nube y las tecnologías emergentes. Nuestra ambición es ser una organización reconocida por la excelencia tecnológica, la innovación responsable, la confianza digital y la capacidad de generar valor sostenible para nuestros clientes, profesionales, accionistas y la sociedad. Entendemos que el crecimiento sostenible solo es posible cuando la innovación se desarrolla bajo principios de calidad, seguridad, privacidad, ética profesional, protección de las personas, sostenibilidad y cumplimiento normativo. Nuestro propósito es ayudar a las organizaciones a innovar, crecer y transformar sus negocios mediante el uso responsable de la tecnología. La Dirección del Grupo asume la responsabilidad última sobre la eficacia del Sistema Integrado de Gestión y se compromete a proporcionar los recursos necesarios para su mantenimiento y mejora, a integrar los principios de esta Política en la estrategia y en las operaciones, a promover una cultura de excelencia, innovación responsable y cumplimiento, y a garantizar su comunicación, comprensión y aplicación efectiva. Todas las personas que forman parte del Grupo Plain Concepts son responsables de contribuir activamente al cumplimiento de esta Política.

Como concreción de este compromiso, nos obligamos a satisfacer los requisitos legales, contractuales y de nuestras partes interesadas que nos son aplicables y a mejorar continuamente el Sistema; a proteger el medio ambiente y prevenir la contaminación; a proteger la confidencialidad, integridad y disponibilidad de la información y la privacidad de los datos personales que tratamos; a proporcionar condiciones de trabajo seguras y saludables, eliminando los peligros y reduciendo los riesgos, con la consulta y participación de nuestros profesionales y de sus representantes; a cumplir nuestras obligaciones de cumplimiento y fomentar una cultura de integridad, respaldando activamente a la función de Compliance; a desarrollar y utilizar la inteligencia artificial de forma responsable; y a mantener la capacidad de seguir prestando nuestros servicios a niveles aceptables ante una disrupción.

Firmado por	Enrique Martínez Alén, CEO · Dirección del Grupo Plain Concepts
Fecha	Según el Anexo B (Firma y aprobación)
Aprobado por	Dirección del Grupo Plain Concepts
Difusión	Pública. Se publica en los canales corporativos internos (Handbook, Teams, Factorial) y en la página web pública del Grupo, y se pone a disposición de clientes, proveedores y otras partes interesadas que la soliciten.

Quiénes somos: contexto organizativo

Plain Concepts nace en 2006 impulsada por cuatro Microsoft Most Valuable Professionals (MVP) con la voluntad de construir una compañía tecnológica de referencia, capaz de atraer y retener talento de excelencia a escala internacional. Nos definimos como una boutique de ingeniería de software y consultoría tecnológica, con vocación de excelencia técnica, cercanía y personalización en el servicio, que sitúa a las personas —clientes y profesionales— en el centro de su forma de trabajar.

El Grupo cuenta con presencia internacional en Alemania, España, Estados Unidos, Países Bajos, Reino Unido y Rumanía, y una plantilla de más de 700 profesionales distribuida en más de 26 centros de entrega («delivery centers»). Nuestra actividad se organiza en cuatro pilares de negocio complementarios:

- **Data:** ordenación, gobierno y explotación de los datos como base de cualquier proceso de transformación.
- **Inteligencia Artificial:** diseño y despliegue de soluciones de IA aplicadas a procesos de negocio, con investigación activa y vigilancia continua del estado del arte.

- **Cloud:** servicios de computación en la nube orientados a la productividad, la sostenibilidad y el impacto del negocio del cliente.
- **Enterprise:** desarrollos a medida para necesidades singulares sin solución estándar disponible en el mercado.

A lo largo de más de 2.400 proyectos hemos prestado servicio a organizaciones de banca y servicios financieros, industria, energía, transporte y administración pública, entre otros, con un enfoque agnóstico respecto a sectores y tecnologías; entre nuestros clientes hay compañías del IBEX-35, grandes multinacionales y organismos públicos, y más del 90 % repite cada año. Somos Global Partner de Microsoft, con distinciones como Partner of the Year en Azure, Inteligencia Artificial, Realidad Mixta y Power Platform, y ampliamos de forma progresiva nuestras capacidades en AWS y Google Cloud Platform para ofrecer una propuesta multicloud. El crecimiento inorgánico —como la incorporación de ApiumHub— y la expansión internacional refuerzan nuestro posicionamiento como socio estratégico de innovación.

Este contexto (mercados, partes interesadas, capacidades y riesgos propios del sector tecnológico) es la base sobre la que se asientan los compromisos de esta Política. Su registro detallado y actualizado se mantiene en REG-04.

Alcance y aplicación de la Política

Los principios y compromisos de esta Política constituyen el marco general de actuación del Grupo Plain Concepts y se aplican a todas las sociedades, filiales, sucursales, establecimientos permanentes, unidades de negocio, centros de trabajo, profesionales y terceros que actúen en su nombre o bajo su dirección, en cualquiera de las geografías en las que operamos.

La aplicación de requisitos específicos derivados de estándares, certificaciones, obligaciones regulatorias o compromisos contractuales se realiza de acuerdo con:

- Los alcances aprobados de los sistemas de gestión implantados en cada momento.
- Las actividades y servicios desarrollados por cada entidad del Grupo.
- Los riesgos identificados en cada línea de negocio y geografía.
- Las obligaciones legales y regulatorias aplicables en cada jurisdicción.
- Los requisitos contractuales asumidos frente a clientes y terceros.
- Las necesidades y expectativas de las partes interesadas pertinentes.

2. Principios de gobernanza

- Una sola información, varias vistas: un hecho se registra una vez y se consulta desde cada perspectiva normativa.
- La evidencia manda: una aprobación no equivale a conformidad; el cumplimiento se demuestra con evidencia verificada.
- Responsabilidad nominal: todo objeto gobernado tiene un propietario identificado.
- Proporcionalidad: la intensidad del control es proporcional al riesgo y al impacto, no uniforme.
- Separación entre ejecución y verificación: quien ejecuta no verifica su propia ejecución.
- Decisión informada: ninguna decisión de gobierno se toma sin la información consolidada que el sistema produce.

Propósito y valores corporativos

Nuestro propósito se apoya en un modelo empresarial basado en la excelencia técnica y el conocimiento especializado; la innovación continua y la orientación al cliente; la confianza digital y la conducta ética y responsable; el desarrollo del talento y la colaboración; y la sostenibilidad como criterio transversal de decisión. Estos principios se concretan en los valores corporativos que definen nuestra forma de actuar:

- **People First:** nuestro principal activo son las personas que forman parte del equipo. Fomentamos un entorno de trabajo flexible, inclusivo y diverso que favorece el desarrollo profesional, el bienestar y la colaboración.
- **Innovación:** impulsamos la innovación como motor de crecimiento y competitividad, nos adaptamos continuamente a los avances tecnológicos y acompañamos a nuestros clientes en sus procesos de transformación.
- **Calidad:** buscamos la excelencia en todo lo que hacemos, con profesionales altamente cualificados y la mejora continua de nuestros procesos.
- **Colaboración ágil:** trabajamos sobre la comunicación, la confianza y la cooperación, con modelos ágiles y eficaces que favorecen la transparencia, la adaptabilidad y la consecución de objetivos comunes.
- **Transparencia:** actuamos con integridad, honestidad y responsabilidad, y mantenemos una comunicación abierta con clientes, empleados, socios y demás partes interesadas.
- **Sostenibilidad:** integramos criterios ambientales, sociales y de buen gobierno en la toma de decisiones para reducir nuestro impacto ambiental y generar valor a largo plazo.

3. Directrices por materia

Calidad y satisfacción del cliente

Los clientes constituyen el centro de nuestra actividad. Nos comprometemos a comprender sus objetivos, necesidades y expectativas; a diseñar, desarrollar y prestar servicios con los más altos estándares de profesionalidad y calidad, alineados con los principios de ISO 9001; a proporcionar soluciones innovadoras que contribuyan a sus objetivos de negocio; a cumplir los requisitos contractuales, regulatorios y legales aplicables; a mantener relaciones basadas en la confianza, la transparencia y la colaboración; y a fomentar la mejora continua de nuestros procesos, servicios y capacidades, incorporando de forma sistemática la voz del cliente. La calidad es una responsabilidad compartida por todas las personas del Grupo, con independencia de su rol, geografía o línea de negocio.

Medio ambiente

Reconocemos nuestra responsabilidad con el entorno y con las generaciones futuras. Promovemos el uso responsable y eficiente de los recursos disponibles; la reducción progresiva de los impactos ambientales asociados a nuestras actividades, en línea con ISO 14001; la integración de criterios ambientales en la toma de decisiones cuando resulte viable y proporcionado, incluida la eficiencia energética de las soluciones cloud e IA que diseñamos para nuestros clientes; la sensibilización de nuestros profesionales respecto a las buenas prácticas ambientales; y la mejora continua de nuestro desempeño ambiental.

Cumplimiento y conducta

La integridad constituye un elemento irrenunciable de nuestra forma de actuar. Actuamos conforme a los principios del Código Ético y mantenemos una cultura basada en el cumplimiento normativo, la responsabilidad corporativa y el respeto a nuestros grupos de interés. Nos comprometemos a cumplir la legislación aplicable en todos los países donde operamos; a mantener mecanismos de prevención, detección

y respuesta frente a conductas irregulares; a identificar, evaluar y gestionar los riesgos de cumplimiento; a mantener un modelo de prevención de riesgos penales; a aplicar diligencia debida proporcional en nuestras relaciones con clientes, proveedores, socios y colaboradores; a prevenir el fraude, la corrupción, el soborno y los conflictos de interés; y a promover una cultura de tolerancia cero frente a cualquier conducta ilícita, garantizando la protección de quienes comuniquen de buena fe. Respetamos asimismo los derechos fundamentales y los principios de actuación responsable, fomentamos una cultura de comunicación abierta que facilite la identificación temprana de riesgos e incumplimientos y protegemos la confianza y la reputación del Grupo. El canal ético y el régimen de incumplimientos se describen en el apartado 7.

Seguridad de la información

La confianza constituye uno de los principales activos del Grupo. Nos comprometemos a promover una gestión responsable de la información y de los activos asociados a la prestación de nuestros servicios; a salvaguardar la confidencialidad, integridad, disponibilidad y trazabilidad de la información de acuerdo con los riesgos identificados y las obligaciones asumidas, en línea con ISO/IEC 27001; a implantar medidas organizativas, técnicas y contractuales proporcionales a la naturaleza de la información; a mantener una cultura corporativa de concienciación y protección de la información; y a mejorar de forma continua nuestras capacidades para responder a un entorno tecnológico en constante evolución. Protegemos asimismo la información confidencial de clientes aplicando el principio de necesidad de conocimiento, con una obligación de confidencialidad que trasciende la duración de la relación contractual. Respetamos los compromisos de confidencialidad adquiridos con clientes, socios y terceros y adoptamos medidas razonables para evitar el acceso, la utilización, la divulgación o la conservación no autorizada de información confidencial.

Seguridad en el ámbito del ENS

Plain Concepts, S.L.U. presta servicios a entidades del sector público y es una de las dos únicas organizaciones certificadas por el Centro Criptológico Nacional (CCN-CERT) para implementar las directrices del Esquema Nacional de Seguridad sobre Microsoft 365 y Azure. El desarrollo formal de la política de seguridad exigida por el Esquema se realiza en el artefacto ENS-DOC-01, al que esta Política se remite. El proceso FP01 proporciona el marco de contexto y riesgos necesario para el cumplimiento de los requisitos del ENS en la categoría que resulte aplicable.

Privacidad y protección de datos

Reconocemos que los datos personales constituyen un activo de especial sensibilidad cuya protección resulta esencial para preservar los derechos y libertades de las personas y la confianza depositada en nuestra organización. Tratamos los datos personales de forma lícita, leal, transparente y responsable, conforme al RGPD y a ISO/IEC 27701; aplicamos los principios de responsabilidad proactiva y privacidad desde el diseño cuando resulte aplicable; integramos la gestión de riesgos de privacidad en las actividades y servicios que lo requieran; adoptamos medidas adecuadas para proteger los datos frente a accesos no autorizados, pérdida, alteración, divulgación o destrucción; y velamos por su adecuada gestión durante todo su ciclo de vida. El Grupo cuenta con un Delegado de Protección de Datos externo (Leasba Consulting).

Inteligencia artificial

La innovación forma parte de nuestra identidad corporativa y constituye uno de los principales motores de crecimiento del Grupo, en línea con nuestro pilar de negocio de Inteligencia Artificial. Promovemos el desarrollo y uso de tecnologías emergentes, incluidos los sistemas de inteligencia artificial, de manera responsable, segura y alineada con nuestros valores y con los requisitos del Reglamento Europeo de Inteligencia Artificial y de ISO/IEC 42001. Integramos criterios de responsabilidad, calidad, seguridad y privacidad en nuestros procesos de innovación; consideramos los riesgos y oportunidades desde las fases iniciales de diseño; promovemos mecanismos de gobernanza a través del Comité de Cumplimiento

Normativo; y favorecemos la supervisión humana, la transparencia y la rendición de cuentas. Informamos a las personas usuarias cuando interactúen con un sistema de IA y etiquetamos los contenidos sintéticos o generados artificialmente. Procuramos adaptar nuestras prácticas a la evolución tecnológica, normativa y sectorial e impulsamos una innovación que contribuya al progreso de nuestros clientes y de la sociedad.

Seguridad y salud en el trabajo

Las personas constituyen el principal motor de innovación y crecimiento de Plain Concepts. Nos comprometemos a mantener entornos de trabajo seguros, saludables, inclusivos y respetuosos, alineados con los principios aplicables de ISO 45001; a promover la participación activa de nuestros profesionales en la mejora de la organización; a favorecer el aprendizaje continuo y el desarrollo profesional; a impulsar una cultura de colaboración, respeto y responsabilidad; a gestionar de forma preventiva los riesgos relacionados con la seguridad y salud de las personas; y a fomentar el bienestar físico, psicológico y social de nuestros equipos.

Continuidad de negocio

Promovemos una gestión basada en riesgos y oportunidades que permita proteger nuestros objetivos estratégicos y fortalecer nuestra capacidad de adaptación. Favorecemos la resiliencia organizativa y operativa mediante el Plan de Continuidad de Negocio del Grupo, que define las actividades críticas, los escenarios de riesgo, los objetivos de recuperación y las estrategias de respuesta, apoyadas en infraestructura cloud de alta disponibilidad, copias de seguridad cifradas y verificadas con pruebas de restauración trimestrales, una política de trabajo «remote-first» y redundancia de los canales de comunicación.

Propiedad intelectual e industrial

El desarrollo de software, productos propios, metodologías y soluciones de IA sitúa a la propiedad intelectual e industrial como un activo estratégico y como una fuente de riesgo que debe gestionarse de forma activa. Nos comprometemos a proteger los activos generados por el Grupo —software, productos propios, metodologías, marcas y demás creaciones— mediante los mecanismos legales oportunos; a respetar los derechos de terceros, incluidos clientes, proveedores, partners tecnológicos y comunidades de código abierto; a establecer criterios claros de titularidad sobre la propiedad intelectual generada en proyectos con clientes, conforme a lo pactado en cada contrato; a gestionar de forma responsable las licencias de software libre y de terceros, verificando su compatibilidad con lo que desarrollamos; a prestar especial atención a los riesgos asociados a la IA generativa —procedencia de los datos de entrenamiento y originalidad del código y los contenidos— antes de incorporarlos a entregables de cliente; y a no tolerar el uso, la reproducción o la distribución no autorizada de obras, software o materiales protegidos. Este compromiso complementa, y no sustituye, las obligaciones de confidencialidad, que responden a una naturaleza jurídica distinta.

Transparencia y rendición de cuentas

La transparencia es un valor nuclear de nuestra cultura de integridad y una condición de la confianza digital. Nos comprometemos a comunicar de forma veraz, oportuna y comprensible con clientes, profesionales, accionistas, proveedores y sociedad, evitando la información engañosa, ambigua o incompleta; a informar a las personas usuarias cuando interactúen con un sistema de IA y a etiquetar los contenidos sintéticos, conforme a las obligaciones de transparencia del Reglamento Europeo de Inteligencia Artificial; a comunicar de forma diligente los incidentes de seguridad o privacidad que puedan afectar a clientes o a sus datos, conforme a la normativa y a los contratos aplicables; a colaborar de forma transparente con autoridades, reguladores, clientes y organismos de certificación; a identificar, comunicar y gestionar los conflictos de interés; y a poner a disposición de las partes interesadas que lo requieran información relevante sobre el desempeño del Sistema, en la medida en que resulte aplicable y proporcionado.

4. Apetito de riesgo y criterios de tolerancia

Gestionamos el Sistema con un enfoque basado en riesgos y oportunidades: evaluamos periódicamente los riesgos relevantes, consideramos las necesidades y expectativas de las partes interesadas, revisamos la eficacia del Sistema y adoptamos decisiones fundamentadas y proporcionales al contexto. El apetito se expresa sobre el nivel de riesgo residual de la escala de DOC-04 y se aplica en REG-10.

Categoría de riesgo	Apetito declarado	Umbral de tolerancia	Qué ocurre al superarlo	Quién puede aceptar el exceso
Calidad y servicio al cliente	Bajo	Residual ≤ Medio	Plan de tratamiento en REG-13 y escalado a la Dirección de SIG	Dirección de SIG; por encima de Alto, Dirección
Ambiental y cumplimiento legal ambiental	Bajo; nulo ante incumplimiento legal	Residual ≤ Medio; ningún incumplimiento legal	Tratamiento inmediato y comunicación a la Dirección	Dirección (no se acepta incumplimiento legal)
Cumplimiento normativo y conducta	Nulo ante conductas ilícitas; bajo en el resto	Ninguna conducta ilícita tolerada; resto residual ≤ Bajo	Investigación por Compliance y comunicación al Comité de Cumplimiento Normativo	No aceptable; resto, Comité de Cumplimiento Normativo
Seguridad de la información	Bajo	Residual ≤ Medio	Plan de tratamiento y escalado al Comité de Seguridad	Comité de Seguridad; por encima de Alto, Dirección
Privacidad y derechos de los interesados	Bajo	Residual ≤ Bajo en tratamientos de alto riesgo	EIPD, consulta al DPO y escalado al Comité de Cumplimiento Normativo	Dirección, con informe del DPO
Sistemas de IA y derechos fundamentales	Nulo en prácticas prohibidas; bajo en el resto	Ninguna práctica prohibida; resto residual ≤ Medio	Suspensión del despliegue y evaluación por el Comité de Cumplimiento Normativo	Comité de Cumplimiento Normativo; alto riesgo, Dirección
Seguridad y salud de las personas	Nulo ante consecuencias graves	Ningún riesgo intolerable ni importante sin medidas	Paralización de la actividad afectada y medidas inmediatas	No aceptable
Continuidad operativa	Bajo	Dentro de los objetivos de recuperación del Plan de Continuidad	Activación del Plan de Continuidad y escalado al Comité de Seguridad	Dirección
Innovación y tecnología	Medio	Residual ≤ Alto, con controles de seguridad y privacidad	Revisión del caso de negocio y de los controles	Dirección de SIG; por encima de Alto, Dirección
Financiero y reputacional	Bajo	Residual ≤ Medio	Escalado a la Dirección	Dirección

5. Estructura de decisión y delegación

La Dirección se reserva las decisiones que fijan el rumbo del Sistema y delega su ejecución en los órganos y roles siguientes; el detalle nominal de órganos, miembros y umbrales se mantiene en REG-01.

Tipo de decisión	Quién decide	Quién debe ser informado	Límite de la delegación
Aprobación y modificación de esta Política	Dirección	Todas las personas del Grupo y partes interesadas	No delegable
Apetito de riesgo y aceptación de riesgo residual por encima del apetito	Dirección	Comité de Seguridad y Comité de Cumplimiento Normativo	No delegable
Aceptación de riesgo residual dentro del apetito	Propietario del riesgo	Dirección de SIG	Hasta el umbral de tolerancia del apartado 4
Objetivos anuales del Sistema y asignación de recursos	Dirección	Dirección de SIG y responsables de área	No delegable
Aprobación de documentos normativos (DOC) y de extensiones	Dirección	Dirección de SIG	Procedimientos e instrucciones: Dirección de SIG
Despliegue de sistemas de IA de alto riesgo	Dirección, con informe del Comité de Cumplimiento Normativo	DPO y Comité de Seguridad	Resto de sistemas de IA: Comité de Cumplimiento Normativo
Gestión de incidentes graves de seguridad o privacidad y activación de continuidad	Comité de Seguridad (sesión de crisis)	Dirección y DPO	Hasta la recuperación del servicio; después, informe a la Dirección
Investigación de comunicaciones del canal ético y medidas resultantes	Función de Compliance	Comité de Cumplimiento Normativo y Dirección	Medidas disciplinarias: Dirección de Personas, con informe de Compliance

Roles y responsabilidades

La eficacia de esta Política depende de una atribución clara de responsabilidades en todos los niveles de la organización:

Rol	Responsabilidad principal
Dirección	Aprueba la Política, asigna recursos y asume la responsabilidad última sobre la eficacia del Sistema. Integra sus principios en la estrategia, impulsa la mejora continua y respalda activamente la función de Compliance y una cultura basada en la integridad, la legalidad y la prevención de riesgos.
Dirección de Sistema Integrado de Gestión (SIG)	Coordina la implantación, el seguimiento y la mejora continua del Sistema en todas las geografías del Grupo, y custodia, actualiza y distribuye esta Política.
Compliance Officer / Función de Cumplimiento	Supervisa el Código Ético, el Modelo de Prevención Penal, el canal ético y la gestión de riesgos de cumplimiento.
Responsable de Seguridad de la Información (CISO)	Dirige la estrategia de seguridad de la información y ciberseguridad, incluida la relación con el ENS y la ISO/IEC 27001.
Delegado de Protección de Datos (DPO)	Supervisa el cumplimiento del RGPD y asesora en materia de privacidad y protección de datos personales.
Comité de Cumplimiento Normativo	Evalúa los riesgos y el cumplimiento normativo de los sistemas de inteligencia artificial desarrollados o utilizados por el Grupo, conforme al Reglamento Europeo de IA e ISO/IEC 42001.
Responsables de área, unidad de negocio o proyecto	Aplican los principios de esta Política en su ámbito y trasladan sus requisitos a clientes, proveedores y equipos.
Todas las personas del Grupo	Conocen, comprenden y aplican esta Política en su actividad diaria y comunican cualquier riesgo o incumplimiento detectado.

6. Compromisos hacia las partes interesadas

Parte interesada	Compromiso asumido	Cómo se demuestra	Dónde se publica
Clientes	Diseñar, desarrollar y prestar servicios con los más altos estándares de calidad; cumplir los requisitos contractuales, regulatorios y legales; proteger la información confidencial confiada; comunicar de forma diligente los incidentes de seguridad o privacidad que puedan afectarles.	Índice de satisfacción y encuestas NPS; índice de recurrencia de clientes; cumplimiento de plazos y requisitos contractuales; certificaciones vigentes.	Contratos, acuerdos de nivel de servicio, web corporativa y procesos de homologación
Personas del Grupo	Mantener entornos de trabajo seguros, saludables, inclusivos y respetuosos; favorecer el aprendizaje continuo y el desarrollo profesional; promover la participación activa en la mejora de la organización.	Encuestas de clima y bienestar; participación en formación; rotación voluntaria por debajo del 15 %.	Handbook, Factorial, Teams y sesiones All Hands
Accionistas	Reporting y alineamiento de objetivos anuales; cumplimiento del presupuesto; información sobre riesgos climáticos, cumplimiento ESG y desempeño ambiental.	Plan estratégico, revisión por la dirección y Estado de Información No Financiera.	Reporting corporativo y EINF
Proveedores y partners	Aplicar medidas proporcionales de diligencia debida; trasladar los requisitos del sistema; respetar los compromisos de confidencialidad.	Evaluación y reevaluación de proveedores; porcentaje de proveedores estratégicos con certificación ambiental.	Contratos y procesos de compra (FP13)
Administraciones públicas y organismos supervisores	Cumplir la legislación aplicable en todos los países donde operamos; colaborar de forma transparente con autoridades, reguladores y organismos de certificación.	Registro de comunicaciones externas; auditorías y homologaciones superadas; certificación CCN-CERT sobre ENS.	Sede electrónica de cada organismo y registro de comunicaciones
Sociedad	Innovación responsable; transparencia sobre el uso de la inteligencia artificial; reducción progresiva del impacto ambiental.	Estado de Información No Financiera; indicadores ESG; comunicaciones UN Global Compact.	Web corporativa y EINF

Objetivos estratégicos e indicadores de desempeño

Esta Política se despliega en objetivos específicos y medibles, revisados anualmente, que se registran en REG-05. A título orientativo, cada ámbito cuenta con objetivos e indicadores como los siguientes:

- **Calidad y satisfacción del cliente:** nivel de satisfacción y cumplimiento de plazos y requisitos contractuales.

- **Seguridad de la información:** número e impacto de incidentes, tiempo de respuesta y cierre de vulnerabilidades, y avance de las certificaciones ENS e ISO/IEC 27001.
- **Privacidad:** brechas de datos personales notificadas y tiempo medio de gestión de los derechos de las personas interesadas.
- **Inteligencia artificial responsable:** porcentaje de proyectos de IA evaluados por el Comité de Cumplimiento Normativo antes de su despliegue.
- **Personas:** participación en formación, resultados de las encuestas de clima y bienestar e indicadores de seguridad y salud.
- **Sostenibilidad:** evolución del consumo de recursos y de la huella ambiental del Grupo.
- **Cumplimiento:** comunicaciones recibidas a través del canal ético y tiempo medio de resolución.

Los objetivos concretos, sus metas anuales y los resultados se revisan en la revisión del Sistema por la Dirección.

7. Incumplimiento de la política

El incumplimiento de esta Política, del Código Ético o de la normativa aplicable se gestiona conforme al Código Ético y al Modelo de Compliance del Grupo. Toda comunicación recibida a través del canal ético es analizada y, en su caso, investigada por la función de Compliance, con los tiempos de respuesta que establece el procedimiento interno correspondiente, garantizando la protección frente a represalias de quienes comuniquen de buena fe.

Para las personas del Grupo, el incumplimiento puede dar lugar a las medidas disciplinarias previstas en la normativa laboral y el convenio colectivo aplicables en cada jurisdicción; para clientes, proveedores y otros terceros, a las medidas previstas en el contrato, incluida su resolución. Los incumplimientos detectados se registran y tratan en REG-13.

Canal ético

El Grupo dispone de un canal ético de información, conforme a la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, a través del cual cualquier persona puede comunicar de buena fe posibles incumplimientos de esta Política, del Código Ético o de la normativa aplicable.

- Está disponible para empleados, clientes, proveedores y otros terceros relacionados con el Grupo.
- Las comunicaciones se gestionan de forma confidencial y admiten, cuando la normativa aplicable lo prevé, la presentación anónima.
- Se garantiza la protección frente a represalias de quienes comuniquen de buena fe, conforme al Código Ético y al Modelo de Compliance del Grupo.
- Toda comunicación es analizada y, en su caso, investigada por la función de Compliance en los plazos del procedimiento interno correspondiente.

8. Vigencia, difusión y revisión

Entrada en vigor	Desde su aprobación y firma
Periodicidad de revisión	Anual
Disparadores de revisión extraordinaria	Cambios relevantes en la estrategia del Grupo, en su contexto operativo, en las necesidades de sus partes interesadas o en los requisitos legales, regulatorios o normativos aplicables
Canales de difusión interna	Handbook, Teams, Factorial, correo corporativo, sesiones All Hands y procesos de acogida de nuevas incorporaciones. Se adapta y, cuando resulta necesario, se traduce a los principales idiomas de las geografías del Grupo para asegurar su comprensión
Disponibilidad externa	La Política es un documento público en su integridad y se publica en la página web corporativa del Grupo
Evidencia de comunicación	Formación periódica adaptada al rol de cada persona, con especial atención a quienes gestionan información de clientes, datos personales o sistemas de IA. Evidencias de formación de alta dirección y de empleados de diciembre de 2025 en REG-08.
Aprobación de revisiones	Toda revisión la aprueba la Dirección y se comunica por los canales indicados
Propiedad y custodia	Dirección de Sistema Integrado de Gestión, que garantiza su custodia, actualización y distribución
Versión controlada	La vigente es la publicada en los canales corporativos oficiales; cualquier copia impresa se considera no controlada

Anexo A. Trazabilidad normativa de este documento

Esta Política forma parte del Sistema de Gobierno, Riesgos y Cumplimiento (GRC) del Grupo y complementa el Código Ético, el Modelo de Prevención Penal y las políticas de Seguridad de la Información, Privacidad, Inteligencia Artificial, Recursos Humanos y Medio Ambiente, entre otras normas corporativas que desarrollan sus principios. Su contenido está alineado con los estándares y marcos siguientes.

Norma / marco	Requisito o cláusula	Cómo lo satisface este documento	Estado
ISO 9001:2015	5.2.1, 5.2.2	Establecimiento, comunicación y disponibilidad de la política de calidad.	Cubierto
ISO 14001:2015	5.2	Política ambiental con sus compromisos obligatorios.	Cubierto
ISO/IEC 27001:2022	5.2, 6.1.2 a); A.5.1	Política de seguridad, criterios de riesgo y políticas temáticas específicas.	Cubierto
ISO/IEC 27701:2019	5.2	Extensión de la política a la protección de la información personal.	Cubierto
ISO/IEC 42001:2023	5.2; A.2	Política de IA y políticas relacionadas.	Cubierto
ISO 37301:2021	5.2, 4.6	Política de compliance, obligaciones y apetito de riesgo de cumplimiento.	Parcial
ISO 45001:2018	5.2	Política de SST, incluidos los compromisos de consulta y participación.	Parcial
ISO 22301:2019	5.2	Política de continuidad de negocio.	Parcial
ENS (RD 311/2022)	Art. 12; org.1	Política de seguridad aprobada por el órgano competente.	Parcial
RGPD (UE 2016/679)	Art. 24.2	Aplicación de políticas de protección de datos apropiadas.	Cubierto
Cyber Essentials	Esquema de certificación (Reino Unido)	Apartado 3, Seguridad de la información: compromiso general de protección.	Parcial
Directiva (UE) 2022/2555 (NIS2)	Arts. 20 y 21, en la medida en que resulte aplicable	Apartados 3, 4 y 5: gobernanza y gestión de riesgos de ciberseguridad.	Parcial
Reglamento (UE) 2024/1689 (Reglamento de IA)	Art. 50	Apartado 3, Inteligencia artificial y Transparencia: información y etiquetado.	Parcial
Ley 2/2023	Art. 5.2 h)	Apartado 7: principios del sistema interno de información y protección del informante.	Parcial
Texto Refundido de la Ley de Propiedad Intelectual (RDLeg. 1/1996)	Libro I, Título VII (programas de ordenador)	Apartado 3, Propiedad intelectual e industrial.	Parcial

Norma / marco	Requisito o cláusula	Cómo lo satisface este documento	Estado
Directiva (UE) 2019/790 (derechos de autor en el mercado único digital)	Arts. 3 y 4 (minería de textos y datos)	Apartado 3, Propiedad intelectual e industrial: datos de entrenamiento de IA.	Parcial
UNE 19601:2017	5.2	Apartados 3 (Cumplimiento y conducta) y 7.	Parcial
Código Ético y Modelo de Compliance del Grupo	Marco interno de integridad	Apartados 3, 5 y 7.	Cubierto

Anexo B. Firma y aprobación

Mediante su firma, el CEO, en representación de la Dirección del Grupo Plain Concepts, aprueba la presente Política y Marco de Dirección y Gobernanza Integrada (DOC-02, versión 1.1), asume los compromisos que contiene y dispone su comunicación, publicación y aplicación en todas las sociedades incluidas en su ámbito. La Política entra en vigor en la fecha de su firma, conforme al apartado 8.

Aprobación	Detalle
Documento	DOC-02 · Política y Marco de Dirección y Gobernanza Integrada
Versión aprobada	1.1
Órgano que aprueba	Dirección del Grupo Plain Concepts
Firmante	D. Enrique Martínez Alén
Cargo	CEO
Lugar y fecha de firma	
Firma	