ANEXO VI – PLAN DE AUDITORÍAS INTERNAS Y EXTERNAS DE COMPLIANCE NEXUS GREEN ENERGY, S.L.

1. OBJETO Y FINALIDAD

El presente Plan tiene por objeto definir la **metodología, alcance, periodicidad, responsabilidades y procedimientos** de las auditorías internas y externas del **Sistema de Cumplimiento y Prevención Penal** de NEXUS GREEN ENERGY, con el fin de **evaluar su eficacia real, detectar desviaciones, verificar la observancia normativa y promover la mejora continua.**

Estas auditorías constituyen una **herramienta esencial de control y transparencia**, en coherencia con los principios establecidos en el **artículo 31 bis del Código Penal**, las normas **UNE 19601**, **ISO 37301** y **ISO 37001**, y los estándares internacionales de **gobernanza ESG y sostenibilidad corporativa (CSRD / Taxonomía UE / GRI / SASB).**

2. PRINCIPIOS RECTORES DE LAS AUDITORÍAS

Toda auditoría de cumplimiento en NEXUS GREEN ENERGY se rige por los siguientes **principios fundamentales**:

a) **Independencia:** los auditores internos o externos actuarán con plena autonomía respecto de las áreas auditadas, sin conflicto de intereses.
b) **Imparcialidad:** los resultados y conclusiones serán objetivos, basados en evidencias verificables y criterios normativos claros.
c) **Trazabilidad:** todas las fases del proceso estarán documentadas para garantizar transparencia y verificabilidad.
d) **Proporcionalidad:** la intensidad de la auditoría se adaptará al nivel de riesgo y criticidad del área auditada.
e) **Periodicidad y continuidad:** las auditorías se realizarán de forma **planificada, recurrente y continua**, no meramente reactiva.
f) **Confidencialidad:** la información obtenida durante la auditoría se considerará confidencial y será utilizada exclusivamente para fines de cumplimiento.
g) **Mejora continua:** los resultados se traducirán en **planes de acción correctiva, preventiva y de refuerzo del sistema.**

3. TIPOLOGÍA DE AUDITORÍAS DE COMPLIANCE

NEXUS GREEN ENERGY contempla dos grandes categorías de auditorías, complementarias entre sí:

3.1. Auditorías Internas

Realizadas por personal propio o dependiente de la **Unidad de Compliance** o de **Auditoría Interna**, con independencia funcional del área auditada.

Objetivos principales:

- Verificar la **efectiva aplicación del Sistema de Compliance Penal** (UNE 19601).
- Comprobar el cumplimiento de políticas internas, protocolos, controles y medidas preventivas.
- Detectar y corregir **deficiencias operativas o de control interno**.
- Evaluar la eficacia de los canales de denuncia y comunicación ética.
- Supervisar la actualización y difusión del **Código Ético** y del **Manual de Cumplimiento**.

3.2. Auditorías Externas

Realizadas por **entidades o consultores externos independientes**, acreditados en sistemas UNE o ISO, con experiencia en compliance, ética corporativa y sostenibilidad.

Objetivos principales:

- Verificar la **conformidad formal y material** del sistema con las normas UNE 19601, ISO 37301 y ISO 37001.
- Obtener una **evaluación objetiva y certificable** ante el Consejo de Administración y los inversores.
- Validar la **idoneidad y eficacia exoneratoria** del modelo conforme al artículo 31 bis CP.
- Evaluar el cumplimiento ESG y de las obligaciones ambientales ETS, CAE, CBAM, GRI y CSRD.

4. ALCANCE DEL PLAN DE AUDITORÍAS

El Plan de Auditorías de Compliance abarca todas las áreas y procesos con potencial riesgo penal, regulatorio o reputacional, incluyendo:

- Área de Trading y Operaciones ETS / CAE / CBAM
- Área Financiera y Fiscal
- Área de Contratación y Proveedores
- Área de Recursos Humanos y Formación Ética
- Área de ESG, Medioambiente y Reporte de Sostenibilidad
- Área de Tecnología y Protección de Datos (IT / RGPD / ENS)
- Área de Comunicación y Gobierno Corporativo

Asimismo, se auditarán los **canales de denuncia (Whistleblowing)**, los **procedimientos de debida diligencia de terceros** y la **eficacia de los controles definidos en la Matriz de Cumplimiento (Anexo IV).**

5. PERIODICIDAD Y PLANIFICACIÓN

Tipo de Auditoría	Frecuencia	Responsable	Alcance
Auditoría Interna General de Compliance	Anual	Compliance Officer / Auditor Interno	Revisión integral UNE 19601 / ISO 37301
Auditoría de Control Penal (Riesgos Art. 31 bis CP)	Anual	Compliance Officer	Evaluación de eficacia del modelo penal
Auditoría del Canal Ético y Whistleblowing	Semestral	Comisión de Ética	Revisión de denuncias, tiempos, garantías
Auditoría del Sistema ESG / Sostenibilidad	Anual	ESG Manager + Auditoría Externa	Cumplimiento CSRD, Taxonomía, GRI
Auditoría de Proveedores Críticos y KYC	Semestral	Compras / Compliance	Revisión de integridad de terceros
Auditoría Externa de Certificación UNE / ISO	Cada 2 años	Entidad Certificadora	Evaluación independiente y certificación
Auditoría Especial / Forense	Según necesidad	Comité Ético + Legal Externo	Casos de sospecha de fraude o delito

6. METODOLOGÍA DE EJECUCIÓN

Todas las auditorías seguirán una **metodología uniforme, estructurada y documentada**, basada en las fases siguientes:

6.1. Planificación

- Identificación de áreas de riesgo y alcance.
- Elaboración del **Programa de Auditoría** (checklists, entrevistas, documentación).
- Designación del equipo auditor y calendario.

6.2. Ejecución

- Revisión documental y análisis de evidencias.
- Entrevistas con responsables de área.
- Pruebas de cumplimiento (muestreo, contraste, validación de controles).
- Detección de desviaciones o incumplimientos.

6.3. Informe de Resultados

- Elaboración del **Informe de Auditoría**, con clasificación de hallazgos según criticidad:
  - **Críticos:** incumplimientos legales o riesgo penal directo.
  - **Mayores:** fallos sustanciales en controles clave.
  - **Menores:** desviaciones administrativas o formales.
- Evaluación global del nivel de madurez del sistema (de 1 a 5).

6.4. Plan de Acción Correctiva

- Definición de medidas correctoras, responsables y plazos.
- Seguimiento de la implantación y verificación de cierre.

6.5. Revisión y Retroalimentación

- Los resultados se presentan a la **Comisión de Ética y Cumplimiento** y al **Consejo de Administración**.
- Se actualizan los **mapas de riesgo y matrices de control** (Anexos II y IV).

7. ROLES Y RESPONSABILIDADES

Cargo / Unidad	Función Principal
Consejo de Administración	Supervisar la ejecución del plan de auditorías y adoptar medidas estratégicas.
Comisión de Ética y Cumplimiento	Aprobar el plan anual de auditorías y supervisar su ejecución.

Cargo / Unidad	Función Principal
Compliance Officer	Dirigir y coordinar auditorías internas; gestionar relaciones con auditores externos.
Auditor Interno	Ejecutar revisiones técnicas, verificar evidencias y elaborar informes.
Departamentos Operativos	Facilitar información, evidencias y colaboración durante las auditorías.
Auditor Externo / Certificador	Emitir dictamen independiente sobre el sistema UNE / ISO y proponer mejoras.

8. DOCUMENTACIÓN Y REGISTRO

Cada auditoría deberá generar un expediente completo que incluirá:

- Programa de auditoría y criterios aplicados.
- Listado de evidencias verificadas.
- Actas de entrevistas.
- Informe de resultados.
- Plan de acción y seguimiento.
- Evidencia documental del cierre de hallazgos.

Todos los registros serán conservados por un periodo mínimo de **5 años** y estarán protegidos conforme al **Reglamento (UE) 2016/679 (RGPD)** y la **Ley Orgánica 3/2018 (LOPDGDD).**

9. EVALUACIÓN DE LA EFICACIA DEL SISTEMA

El **Compliance Officer** elaborará un **Informe de Evaluación Anual**, que consolidará:

- Número total de auditorías realizadas.
- Porcentaje de cumplimiento de controles críticos.
- Tipología y frecuencia de hallazgos.
- Nivel de madurez del sistema (Escala 1 a 5).
- Grado de implantación de planes correctivos.
- Propuestas de mejora y evolución.

Dicho informe se presentará al **Consejo de Administración** y servirá de base para la **revisión anual del Sistema de Compliance.**

10. COMUNICACIÓN Y TRANSPARENCIA

Los resultados relevantes de las auditorías, sin revelar información confidencial, podrán incluirse en:

- El **Informe Anual de Compliance y Ética Corporativa.**
- El **Reporte de Sostenibilidad (ESG / CSRD)**.
- Comunicaciones institucionales a inversores o stakeholders.

La transparencia en la rendición de cuentas fortalece la **reputación ética y la legitimidad pública** de NEXUS GREEN ENERGY.

11. MEJORA CONTINUA

El **Plan de Auditorías** es un documento dinámico. Será **revisado anualmente** para:

- Adaptarse a nuevas leyes, regulaciones o estándares internacionales.
- Incorporar lecciones aprendidas y buenas prácticas.
- Ajustarse a cambios estructurales o estratégicos de la organización.

El objetivo es garantizar que el sistema de cumplimiento evolucione con la misma agilidad que el entorno normativo y operativo en el que opera la compañía.

12. CONCLUSIÓN

El **Plan de Auditorías Internas y Externas de Compliance** constituye la piedra angular del **mecanismo de control y verificación independiente** de NEXUS GREEN ENERGY.

Permite asegurar que el cumplimiento normativo no es solo un principio declarado, sino una **práctica verificable, medible y auditada con rigor técnico y transparencia.**

"Auditar es demostrar, con hechos, que la integridad corporativa no se presume: se prueba."

Le saluda atentamente,

En Madrid a 15 de octubre de 2025

La Junta de Socios de Nexus Green Energy, S.L.