GRANSOLAR GROUP

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO DOC.: GGR-CO-POL-0005-A3
VERSIÓN: A3
FECHA: 25/03/2026

RESUMEN:

TÍTULO	Política de Seguridad de la Información
ÁMBITO DE APLICACIÓN	Grupo Gransolar (tal y como se define a continuación)
DISCIPLINA	Corporativo
CATEGORÍA	Política
ELABORADO POR	Responsable Departamento de IT (tal y como se define a continuación)
DEPARTAMENTO RESPONSABLE	Departamento de IT
FECHA DE APROBACIÓN	25/03/2026
ÓRGANO DE APROBACIÓN	Consejo de Administración (tal y como se define a continuación)
VERSIÓN QUE SUSTITUYE	A2
VERSIÓN ACTUAL	A3
USO	Público

HISTÓRICO DE VERSIONES:

VERSIÓN	FECHA	ELABORADO POR	CAMBIOS REALIZADOS	REVISADO POR
A1	15/09/2021	Responsable Departamento de IT	Creación	Consejo de Administración
A2	17/12/2024	Responsable Departamento de IT	Unificación de políticas	Departamento de Gobernanza
A3	25/03/2026	Responsable Departamento de IT	Actualización para alineación con la última versión de la ISO 27001 y con la Directiva NIS2	Departamento de Gobernanza

HISTÓRICO DE APROBACIONES:

VERSIÓN	FECHA	APROBADO POR
A1	15/09/2021	Consejo de Administración
A2	17/12/2024	Consejo de Administración
A3	25/03/2026	Consejo de Administración

ÍNDICE

1. GLOSARIO

A los efectos de la presente política de seguridad de la información (en adelante, la "**Política**"):

(i) "**Código de Comercio**" significará el Código de Comercio español;

(ii) **"Comité de ESG**" significará el órgano consultor del Consejo de Administración, encargado de gestionar y supervisar las cuestiones de ESG (ambientales, sociales y de gobierno corporativo) de Grupo Gransolar, previo a su aprobación o presentación final al Consejo de Administración;

(iii) "**Consejo de Administración**" significará el Consejo de Administración de Grupo Gransolar, S.L.;

(iv) "**Departamento de Gobernanza**" significará el departamento de gobernanza de Grupo Gransolar;

(v) "**Departamento de IT**" significará el departamento de tecnología de la información (IT) de Grupo Gransolar;

(vi) "**Directiva NIS2**" significará la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y se deroga la Directiva (UE) 2016/1148;

(vii) "**Estatutos Sociales**" significará los estatutos sociales de Grupo Gransolar, S.L.;

(viii) "**Grupo**" significará un grupo de sociedades en el sentido previsto en el artículo 42 del Código de Comercio, es decir, un grupo de sociedades que, conforme a lo dispuesto en el referido artículo, se encuentre bajo el control, directo o indirecto, de una sociedad dominante;

(ix) "**Grupo Gransolar**" significará el Grupo cuya sociedad dominante es Grupo Gransolar, S.L.;

(x) "**Incidente de Seguridad de la Información**" (colectivamente, los "**Incidentes de Seguridad de la Información**") significará cualquier evento que comprometa o pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de la Información o de los Sistemas de Información de Grupo Gransolar, o que afecte a la prestación de los servicios soportados por dichos sistemas;

(xi) "**Incidente Significativo de Seguridad de la Información**" significará cualquier Incidente de Seguridad de la Información que tenga, o pueda tener, un impacto significativo en la prestación de los servicios de Grupo Gransolar o en la seguridad de sus Sistemas de Información, atendiendo, entre otros factores, al número de usuarios afectados, la duración del incidente, su alcance geográfico, la gravedad de la alteración de los servicios o el impacto económico o reputacional que pueda ocasionar;

(xii) "**Información**" significará cualquier dato o conjunto de datos, con independencia de su formato, soporte o medio de transmisión, que sea generado, recopilado, tratado, almacenado o transmitido por Grupo Gransolar en el desarrollo de sus actividades, incluyendo, entre otros, la información (a) relativa al propio Grupo Gransolar, sus administradores, directivos y empleados, así como aquella relativa a proveedores, contratistas, subcontratistas, socios comerciales, clientes u otros terceros, o facilitada por estos a Grupo Gransolar y (b) que tenga la consideración de datos personales, de conformidad con la normativa aplicable en materia de protección de datos, en particular el Reglamento de Protección de Datos y la Ley de Protección de Datos;

(xiii) "**ISO 27001**" significa la norma internacional ISO/IEC 27001 que establece los requisitos para implantar, mantener y mejorar un sistema de gestión de seguridad de la información;

(xiv) "**Ley de Protección de Datos**" significará la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales;

(xv) "**Macro Política Corporativa**" significará la macro política corporativa de corporativo de Grupo Gransolar;

(xvi) "**ODS**" significará los Objetivos de Desarrollo Sostenible establecidos en la Agenda 2030 para el Desarrollo Sostenible;

(xvii) "**Plan Director de Gobernanza**" significará el plan director de gobernanza de Grupo Gransolar, S.L.;

(xviii) "**Reglamento de Protección de Datos**" significará el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE;

(xix) "**Sistemas de Información**" significará el conjunto de sistemas, procesos, tecnologías, aplicaciones, dispositivos, redes, soportes, infraestructuras y servicios de tecnologías de la información y las comunicaciones y demás recursos que permiten la creación, recopilación, tratamiento, almacenamiento, transmisión o protección de la Información utilizada por Grupo Gransolar, tanto en entornos físicos como digitales;

(xx) "**Usuario**" (colectivamente, "**Usuarios**") significará cualquier:

(a) empleado de las sociedades que integran Grupo Gransolar, entendiéndose por tales cualesquiera personas vinculadas a dichas sociedades mediante una relación laboral, mercantil, formativa o cualquier otra relación jurídica de naturaleza análoga;

(b) directivo de las sociedades que integran Grupo Gransolar;

(c) administrador de las sociedades que integran Grupo Gransolar;

(d) contratista, proveedor, socio de *joint venture*, cliente, consultor o tercero autorizado, así como sus respectivos empleados;

(e) cualquier personal externo o eventual;

que acceda o utilice Información o Sistemas de Información de Grupo Gransolar.

2. INTRODUCCIÓN

Grupo Gransolar basa su modelo de gestión en la excelencia operativa, dando respuesta a las necesidades y expectativas de sus grupos de interés, aportando valor a la sociedad y promoviendo un desarrollo sostenible en sus dimensiones social, económica y ambiental.

En este contexto, el sistema de gobierno corporativo de Grupo Gransolar se articula a través de un conjunto de normas internas (el "**Sistema Normativo Interno**") entre las que se encuentran las políticas corporativas, las cuales constituyen un elemento esencial para (i) garantizar el cumplimiento de la normativa aplicable, (ii) establecer directrices claras para el desarrollo de las actividades y (iii) favorecer la homogeneización y eficiencia de los procesos internos.

El Sistema Normativo Interno se inspira en los más altos estándares internacionales en materia de sostenibilidad, ética empresarial y buen gobierno. En particular (y a título meramente ejemplificativo), como miembro participante del Pacto Mundial de las Naciones Unidas, Grupo Gransolar promueve los ODS y asume activamente su responsabilidad como agente de cambio en materia de sostenibilidad.

Asimismo, Grupo Gransolar mantiene un firme compromiso con:

(i) el respeto y la protección de los Derechos Humanos, adoptando una posición preventiva y de diligencia debida frente a posibles vulneraciones en los territorios en los que opera (este compromiso se extiende a todos los grupos de interés de Grupo Gransolar, poniendo a su disposición un canal de denuncias); y

(ii) la promoción de los más altos estándares de transparencia, ética empresarial y rendición de cuentas, aplicando una política de tolerancia cero frente a cualquier conducta contraria a lo establecido en el Sistema Normativo Interno y extendiendo estos principios a lo largo de toda su cadena de valor.

En coherencia con lo anterior, Grupo Gransolar impulsa una cultura organizativa basada en la anticipación normativa, promoviendo la adopción temprana de nuevas regulaciones, así como la incorporación de directrices, estándares y recomendaciones emitidas por organismos internacionales de referencia.

3. OBJETO Y FINALIDAD

El objeto de la presente Política es establecer los principios, criterios y directrices que deben regir la actuación de Grupo Gransolar en materia de seguridad de su Información y sus Sistemas de

Información (activos estratégicos para Grupo Gransolar que, por ende, deben ser protegidos frente a amenazas tales como errores, sabotajes, terrorismo, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio y desastres naturales), todo ello con el fin de:

(i) promover en Grupo Gransolar:

(a) una gestión responsable y homogénea de la Información y de los Sistemas de Información, que cumpla con lo dispuesto en la normativa en materia de protección de datos y ciberseguridad, en particular el Reglamento de Protección de Datos, la Ley de Protección de Datos y la Directiva NIS2 (la "**Normativa de Datos y Ciberseguridad**"), y que esté alineada con estándares de referencia en materia de seguridad de la información y ciberseguridad vigentes en cada momento, tales como la ISO 27001;

(b) un entorno seguro para el uso y manejo de la Información y los Sistemas de Información en todos los niveles organizacionales;

(ii) garantizar la seguridad, calidad, resiliencia y continuidad de los Sistemas de Información y de los servicios soportados por los mismos; y

(iii) reducir al máximo las posibilidades de que se produzcan Incidentes de Seguridad de la Información y, en caso de que se produzcan, minimizar su impacto.

4. ÁMBITO DE APLICACIÓN

4.1. ÁMBITO DE APLICACIÓN OBJETIVO

La presente Política será de aplicación a toda la Información y los Sistemas de Información de Grupo Gransolar.

4.2. ÁMBITO DE APLICACIÓN SUBJETIVO

La presente Política será de aplicación a (y, por ende, será de obligatorio cumplimiento por) los Usuarios.

4.3. ÁMBITO DE APLICACIÓN GEOGRÁFICO

La presente Política será aplicable en todos los países en los que Grupo Gransolar desarrolle sus actividades, sin perjuicio de las adaptaciones que resulten necesarias para dar cumplimiento a la normativa local aplicable en cada jurisdicción.

5. PRINCIPIOS GENERALES

En el desarrollo de sus actividades, Grupo Gransolar actuará conforme a los siguientes principios generales:

(i) Cumplimiento normativo: Grupo Gransolar desarrollará sus actividades de conformidad con (a) la normativa aplicable en cada jurisdicción en la que opere y (b) lo dispuesto en el Sistema Normativo Interno, promoviendo una cultura de cumplimiento y de tolerancia cero frente a conductas contrarias a la legalidad o a sus normas internas.

(ii) Integración en la estrategia y en la toma de decisiones: Grupo Gransolar integrará los principios recogidos en todos los documentos de su Sistema Normativo Interno (incluida, entre otros, la presente Política) en su estrategia corporativa, en sus procesos de toma de decisiones y en la gestión de sus actividades y operaciones.

(iii) Gestión basada en riesgos: Grupo Gransolar aplicará un enfoque preventivo y basado en riesgos, promoviendo la identificación, evaluación, mitigación y seguimiento de los riesgos asociados al ámbito de actuación de todos los documentos de su Sistema Normativo Interno (incluida, entre otros, la presente Política).

(iv) Responsabilidad y rendición de cuentas: Grupo Gransolar promoverá una actuación responsable, transparente y trazable, estableciendo mecanismos adecuados de supervisión, control y seguimiento que permitan garantizar la correcta aplicación de todos los documentos de su Sistema Normativo Interno (incluida, entre otros, la presente Política).

(v) Mejora continua: Grupo Gransolar fomentará la revisión y mejora continua de sus procesos, herramientas y sistemas de gestión, adaptándose a la evolución normativa, tecnológica y de su entorno de negocio.

(vi) Formación y sensibilización: Grupo Gransolar promoverá la formación, comunicación y sensibilización de todos los documentos de su Sistema Normativo Interno (incluida, entre otros, la presente Política), con el fin de garantizar su adecuada comprensión y cumplimiento por su correspondiente ámbito de aplicación subjetivo.

(vii) Extensión a la cadena de valor: Grupo Gransolar promoverá la aplicación de los principios recogidos en todos los documentos de su Sistema Normativo Interno (incluida, entre otros, la presente Política) en sus relaciones con socios comerciales, proveedores, contratistas y demás terceros, cuando resulte apropiado en función de la naturaleza de la relación.

(viii) Respeto a los estándares internacionales: Grupo Gransolar orientará su actuación conforme a estándares, directrices y buenas prácticas internacionales reconocidas en materia de sostenibilidad, ética empresarial y buen gobierno.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Además de los principios generales establecidos en el Apartado 5 anterior (los cuales regirán todas las actividades de Grupo Gransolar en general), con respecto a la Información y los Sistemas de Información, Grupo Gransolar actuará conforme a los siguientes principios:

(i) Seguridad: Grupo Gransolar desarrollará y mantendrá un sistema de gestión de seguridad de la Información basado en estándares internacionales reconocidos.

(ii) Cultura de seguridad: Grupo Gransolar promoverá una cultura de seguridad de la Información en todos los niveles de la organización.

(iii) Disponibilidad: Grupo Gransolar garantizará que la Información y Sistemas de Información puedan ser utilizados en los tiempos y forma requerida.

(iv) Confidencialidad: Grupo Gransolar se asegurará de que solo las personas debidamente autorizadas accedan a la Información y Sistemas de Información.

(v) Integridad: Grupo Gransolar adoptará las medidas necesarias para proteger la Información frente a modificaciones no autorizadas o indebidas, garantizando su exactitud y fiabilidad.

(vi) Autenticidad: Grupo Gransolar se asegurará de que la fuente de la que procede la Información es propietaria de ésta y es quien dice ser.

(vii) Legalidad: Grupo Gransolar tratará la Información y los Sistemas de Información de acuerdo con la Normativa de Datos y Ciberseguridad.

(viii) Gestión de riesgos de seguridad de la Información: Grupo Gransolar adoptará un enfoque basado en la gestión de riesgos para la protección de la Información y de los Sistemas de Información, mediante la implementación de medidas técnicas, operativas y de organización adecuadas y proporcionadas para:

(a) proteger y mantener la confidencialidad, integridad y disponibilidad de la Información y los Sistemas de Información;

(b) detectar de manera continua los riesgos de que se produzcan Incidentes de Seguridad de la Información (colectivamente los "**Riesgos**");

(c) prevenir o minimizar las repercusiones de los Incidentes de Seguridad de la Información; y

(d) garantizar un nivel de seguridad de la Información y los Sistemas de Información adecuado en relación con los Riesgos detectados;

colectivamente, las "**Medidas de Seguridad**", que aborden, entre otros, los siguientes ámbitos:

(a) el análisis y la gestión de Riesgos;

(b) la prevención, detección y gestión de Incidentes de Seguridad de la Información;

(c) la continuidad de las operaciones y la recuperación ante incidentes que afecten a los Sistemas de Información;

(d) la seguridad en la cadena de suministro y en las relaciones con proveedores y terceros;

(e) la seguridad en la adquisición, desarrollo, mantenimiento y operación de los Sistemas de Información;

(f) la evaluación periódica de la eficacia de las Medidas de Seguridad adoptadas;

(g) la formación, concienciación y promoción de buenas prácticas en materia de ciberseguridad;

(h) el uso adecuado de mecanismos de protección de la Información, incluyendo, cuando resulte apropiado, medidas de cifrado y criptografía;

(i) la gestión de identidades y accesos, así como el uso de mecanismos de autenticación reforzada y comunicaciones seguras; y

(j) la seguridad de recursos humanos.

(ix) Seguridad por diseño y por defecto: el principio de seguridad de la Información se integrará desde las fases iniciales de diseño, desarrollo, adquisición e implementación de los Sistemas de Información.

(x) Responsabilidad: todos los Usuarios serán responsables de proteger la Información y de cumplir las Medidas de Seguridad.

(xi) Seguridad en la cadena de suministro: tal y como se mencionaba anteriormente, Grupo Gransolar adoptará, entre otras medidas, Medidas de Seguridad destinadas a garantizar que los proveedores, contratistas y terceros que tengan acceso a Información o Sistemas de Información de Grupo Gransolar, o que participen en la prestación de servicios tecnológicos o digitales, cumplan con estándares adecuados de seguridad de la Información y ciberseguridad (estas Medidas de Seguridad deberán aplicarse teniendo en cuenta, entre otros factores, las vulnerabilidades específicas de los proveedores y prestadores de servicios, la calidad y seguridad de los productos o servicios suministrados, así como las prácticas de ciberseguridad aplicadas por dichos proveedores, incluidos, cuando resulte aplicable, sus procedimientos de desarrollo seguro). A tal efecto, Grupo Gransolar promoverá la evaluación de los Riesgos asociados a dichos terceros (siempre y cuando los mismos vayan a suministrar bienes y/o servicios que supongan un impacto en los servicios o Sistemas de Información de Grupo Gransolar) y, cuando resulte necesario, se establecerán y documentarán requisitos específicos de seguridad de la Información en los correspondientes acuerdos contractuales con dichos proveedores o terceros (estos requisitos serán acordados de mutuo acuerdo), con el fin de mitigar los Riesgos identificados y garantizar el cumplimiento de la presente Política y de la normativa aplicable.

(xii) Mejora continua de las Medidas de Seguridad: Grupo Gransolar revisará y mejorará de forma continua las Medidas de Seguridad mediante evaluaciones, auditorías y revisiones periódicas.

(xiii) Resiliencia: Grupo Gransolar adoptará medidas destinadas a garantizar la capacidad de sus Sistemas de Información para resistir, adaptarse y recuperarse ante incidentes o interrupciones.

(xiv) Clasificación de la Información: Grupo Gransolar establecerá criterios para la clasificación de la Información en función de su sensibilidad, valor y criticidad para la organización, garantizando que dicha Información sea tratada y protegida de acuerdo con su nivel de clasificación.

(xv) Uso seguro de la Información y de los Sistemas de Información: Grupo Gransolar se asegurará de que los que los Usuarios:

(a) hagan buen uso de la Información y los Sistemas de Información en el desarrollo de sus funciones, obligaciones y responsabilidades, sin comprometer la seguridad de dicha Información y Sistemas de Información;

(b) adopten, implementen y mantengan de forma continua medidas técnicas, organizativas y administrativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la Información que les haya proporcionado Grupo Gransolar;

(c) cumplan con la Normativa de Datos y Ciberseguridad y los estándares de seguridad aplicables;

(d) notifiquen cualquier Incidente de Seguridad de la Información a Grupo Gransolar; y

(e) devuelvan a Grupo Gransolar (o destruyan) la Información recibida una vez finalizada su relación contractual con la correspondiente sociedad de Grupo Gransolar.

7. CONTROL DE CUMPLIMIENTO Y RESPUESTA ANTE INCUMPLIMIENTOS

7.1. CONTROL DE CUMPLIMIENTO

7.1.1. El responsable del Departamento de IT coordinará evaluaciones periódicas destinadas a verificar el grado de cumplimiento de la presente Política por parte de los Usuarios.

7.1.2. Asimismo, se llevarán a cabo auditorías, tanto internas como externas, con el fin de verificar el cumplimiento de la presente Política, al menos una vez al año o siempre que se produzcan cambios sustanciales en los Sistemas de Información.

7.1.3. Los resultados de dichas evaluaciones y auditorías podrán dar lugar a la adopción de medidas correctivas o de mejora cuando resulte necesario.

7.2. EXCEPCIONES

Toda excepción a lo dispuesto en la presente Política deberá ser reportada al responsable del Departamento de IT, o la función responsable de la seguridad de la Información designada por Grupo Gransolar en cada momento, que analizará y evaluará el riesgo que dicha excepción podría suponer para Grupo Gransolar y, en base a la categorización de dicho riesgo, el mismo deberá ser asumido por el peticionario de la excepción junto con los responsables del negocio.

7.3. INCUMPLIMIENTOS

7.3.1. Todo Usuario que tenga conocimiento de:

(i) situaciones sospechosas o anómalas relacionadas con la Información y/o Sistema de Información;

(ii) Incidentes de Seguridad de la Información; o

(iii) incumplimientos de la presente Política o de las medidas de Seguridad;

deberá informar de ello a la persona responsable de la seguridad de la Información designada por Grupo Gransolar en cada momento.

7.4. El incumplimiento de la presente Política será considerado como una falta grave y podrá dar lugar a:

(i) la aplicación del régimen disciplinario que resulte de aplicación, sin perjuicio de otras responsabilidades legales o contractuales que pudieran derivarse; y

(ii) en su caso, la terminación de la relación contractual de la parte incumplidora con la correspondiente sociedad de Grupo Gransolar.

7.5. Los Incidentes Significativos de Seguridad de la Información deberán ser gestionados y, en su caso, notificados sin demora indebida a las autoridades competentes de conformidad con la Normativa de Datos y Ciberseguridad, de conformidad con los plazos establecidos en la misma.

7.6. Cuando resulte procedente, Grupo Gransolar podrá asimismo informar a los destinatarios de sus servicios sobre aquellos Incidentes Significativos que puedan afectar negativamente a la prestación de dichos servicios.

8. NORMATIVA INTERNA VINCULADA

8.1. JERARQUÍA ASCENDENTE

La presente Política forma parte del Sistema Normativo Interno de Grupo Gransolar, y se sitúa jerárquicamente por debajo de las siguientes normas corporativas, de las que depende y en cuyo desarrollo se dicta:

(i) los Estatutos Sociales;

(ii) el Plan Director de Gobernanza; y

(iii) la Macro Política Corporativa.

8.2. JERARQUÍA DESCENDENTE

8.2.1. La presente Política se desarrolla mediante un manual de seguridad del usuario, en el cual se establecen los requisitos (basados en las mejores prácticas de mercado y alineados con las necesidades específicas de Grupo Gransolar) que deben cumplir todos los Usuarios con respecto a la Información y los Sistemas de Información de Grupo Gransolar.

8.2.2. Sin perjuicio de lo anterior, la presente Política podrá desarrollarse mediante cualquier otro procedimiento, protocolo u otra norma interna que concrete su aplicación práctica.

8.2.3. En caso de contradicción entre la presente Política y normas internas de rango inferior, prevalecerá lo dispuesto en esta Política, sin perjuicio de lo establecido en la normativa legal aplicable o en normas internas de rango superior.

8.3. MISMO NIVEL JERÁRQUICO

En caso de que existan en Grupo Gransolar políticas corporativas específicas que, dependiendo de la misma Macro Política Corporativa, regulen materias relacionadas con el objeto de la presente Política (incluidas aquellas cuya adopción resulte obligatoria conforme a la normativa aplicable en una jurisdicción específica), dichas políticas deberán:

(i) respetar los principios y directrices generales establecidos en la correspondiente Macro Política Corporativa; y

(ii) aplicarse de forma coordinada con la presente Política.

9. DEPARTAMENTO RESPONSABLE

El departamento responsable de la presente Política es el Departamento de IT.

10. COMPROMISO DEL CONSEJO DE ADMINISTRACIÓN

El Consejo de Administración asume la responsabilidad de:

(i) aprobar las Medidas de Seguridad y supervisar su implementación;

(ii) garantizar la disponibilidad de los recursos necesarios para la implementación, mantenimiento y mejora continua de las Medidas de Seguridad.; y

(iii) fomentar a todos los niveles organizativos de Grupo Gransolar el cumplimiento de los principios de seguridad establecidos en la presente Política.

11. CAMBIO CLIMÁTICO

11.1. Grupo Gransolar tiene en consideración los riesgos y oportunidades derivados del cambio climático en el análisis del contexto de sus Sistemas de Información y en la gestión de los Riesgos asociados a los mismos.

11.2. En particular, Grupo Gransolar tendrá en cuenta los posibles impactos derivados de fenómenos climáticos extremos u otras condiciones ambientales que puedan afectar a la disponibilidad, integridad o resiliencia de sus Sistemas de Información y de las infraestructuras tecnológicas que los soportan.

12. COMUNICACIÓN Y SENSIBILIZACIÓN

12.1. COMUNICACIÓN INTERNA

La presente Política será publicada en la *intranet* corporativa de Grupo Gransolar, de modo que sea (i) difundida entre y (ii) accesible para, todos sus empleados.

12.2. COMUNICACIÓN EXTERNA

La presente Política será publicada en las páginas web de Grupo Gransolar, para que sus grupos de interés puedan acceder a la misma.

12.3. SESIBILIZACIÓN

Grupo Gransolar formará a todos sus empleados, directivos y administradores sobre el contenido de la presente Política, garantizando de este modo un adecuado nivel de concienciación y capacitación en materia de seguridad de la Información y de los Sistemas de Información.

13. REVISIÓN Y ACTUALIZACIÓN

13.1. La presente Política será revisada y – en su caso – actualizada, cada tres (3) años por el Departamento de IT, en coordinación con el Departamento de Gobernanza.

13.2. Sin perjuicio de lo anterior, la presente Política podrá ser revisada y, en su caso, actualizada con carácter anticipado cuando (i) se produzcan cambios normativos, organizativos o en el perfil de los riesgos asociados a su ámbito de aplicación, o (ii) el Departamento de IT y/o el Departamento de Gobernanza lo consideren oportuno, por cualquier otra circunstancia.

13.3. En cualquier caso, toda propuesta de modificación deberá ser reportada al Comité de ESG, que será el encargado de elevar dicha propuesta al Consejo de Administración para su aprobación.

14. APROBACIÓN

La presente Política ha sido aprobada por el Consejo de Administración de Grupo Gransolar, S.L., como parte de su potestad general e indelegable de aprobar las políticas y estrategias generales de Grupo Gransolar.

15. DISPOSICIONES ADICIONALES

La presente Política deberá interpretarse de conformidad con la normativa aplicable (incluida la Normativa de Datos y Ciberseguridad) y el Sistema Normativo Interno.

GRANSOLAR GROUP

Avda. de la Transición Española, 32

Parque Empresarial Omega, Edificio A, 4ª Planta

28108, Alcobendas (Madrid), España

+34 917 364 248 | group@gransolar.com