POLÍTICA INTEGRADA DE GOBERNANZA, CONFORMIDAD Y RESPONSABILIDAD EMPRESARIAL GRUPO SAFETY21

Rev.	Descripción de la modificación	Fecha
00	Primera emisión	21/12/2017
01	Segunda emisión	13/01/2020
02	Tercera emisión	22/11/2021
03	Aspectos específicos sobre la privacidad	06/07/2022
04	Incorporación de aspectos relativos a la continuidad operativa	20/10/2022
05	Incorporación de aspectos relativos a las certificaciones faltantes (SA 8000, ISO 37001, ISO 45001, UNI PDR125, ISO 18295-1)	30/06/2024
06	Revisión del marco normativo	09/10/2024
07	Resumen general e integración de todos los sistemas de gestión de Safety21	27/05/2025
08	Ampliación del ámbito de aplicación al Grupo Safety21 – Certificación B Corp	22/09/2025
09	Incorporación de la función de conformidad	18/11/2025
10	Información detallada sobre las empresas del Grupo	01/12/2025
11	Adaptación a la norma UNI ISO 37001:2025	16/02/2026
12	Revisión de la gobernanza integrada, el marco normativo y las medidas de control de la privacidad, ciberseguridad e inteligencia artificial	20/10/2026

Roberto Campisi
Presidente



ÍNDICE

1. INTRODUCCIÓN ---- 3
2. OBJETIVO Y ÁMBITO DE APLICACIÓN ---- 3
3. VALORES ---- 5
4. CALIDAD Y PUNTOS DE CONTACTO PARA EL CLIENTE (UNI EN ISO 9001:2015, UNI EN ISO 18295-1:2017): ---- 6
5. SALUD Y SEGURIDAD EN EL TRABAJO (UNI EN ISO 45001:2023) ---- 7
6. MEDIO AMBIENTE (UNI EN ISO 14001:2015) – B CORP ---- 8
7. CIBERSEGURIDAD, RESILIENCIA DIGITAL Y GESTIÓN DE SERVICIOS ---- 8
8. 8. PROTECCIÓN DE DATOS PERSONALES Y GOBERNANZA DE LA INFORMACIÓN ---- 10
9. IGUALDAD DE GÉNERO (UNI PDR 125:2022) – B CORP ---- 11
10. ANTICORRUPCIÓN (UNI ISO 37001:2025) ---- 12
11. CONTINUIDAD OPERATIVA (ISO 22301:2019) ---- 13
12. SISTEMA DE CONSERVACIÓN (SDC) ---- 14
13. RESPONSABILIDAD SOCIAL (SA8000) – B CORP ---- 14
14. COMUNICACIÓN Y DIFUSIÓN ---- 15
15. ACTUALIZACIÓN Y REVISIÓN ---- 15

1. INTRODUCCIÓN

Safety21 constituye actualmente un grupo de empresas capaz de cumplir con los más altos estándares de servicio en apoyo de las administraciones públicas.
La empresa se compromete a alcanzar la excelencia en todas sus actividades, adoptando prácticas sostenibles, éticas y responsables. Creemos que un enfoque integrado y global es fundamental para garantizar la plena satisfacción de nuestros clientes, proteger el medio ambiente, promover el bienestar de nuestro personal y asegurar la sostenibilidad a largo plazo de nuestras actividades.

Uno de los principios fundamentales de Safety21 es la ética empresarial, que promueve valores de lealtad, honestidad y respeto, y que sirve de guía para nuestro compromiso social. En este contexto, la empresa se propone reforzar los principios de su Código Ético y apoyar activamente todas las iniciativas que contribuyan a consolidar las normas y los estándares de conducta aplicables a todo el personal, con el fin de evitar cualquier perjuicio para la propia empresa, incluso en términos de imagen.

Garantiza el cumplimiento de la normativa vigente, tanto en las relaciones entre particulares como frente a la Administración Pública, respetando las medidas de control recogidas en el Modelo Organizativo previsto en el Decreto Legislativo italiano número 231/2001.

Asimismo, la empresa se compromete a mejorar continuamente su Sistema de gestión anticorrupción y garantiza la autoridad (definida mediante las responsabilidades atribuidas a esta función y comunicadas a todo el personal de la empresa) y la independencia de la Función de conformidad para la prevención de la corrupción, designada por la Alta Dirección.

2. OBJETIVO Y ÁMBITO DE APLICACIÓN

La dirección de Safety21 está convencida de que el proceso de mejora continua constituye un elemento fundamental para alcanzar la excelencia a la hora de combinar el crecimiento de la empresa con:

- ✓ altos estándares de calidad, resiliencia y eficiencia de los servicios prestados;
- ✓ la protección de las expectativas y las necesidades de las partes interesadas pertinentes;
- ✓ el respeto por el medio ambiente;
- ✓ la protección de la salud y la seguridad de los trabajadores;
- ✓ la protección de la información y de los datos personales;
- ✓ valorización del capital humano, respeto de los derechos y búsqueda del bienestar de los empleados.

Las certificaciones y las normas voluntarias constituyen herramientas de apoyo al modelo de gobernanza y control, pero no sustituyen el análisis de las disposiciones legales aplicables ni limitan el alcance de las obligaciones de la empresa. El Grupo identifica y actualiza periódicamente los requisitos normativos aplicables en función de las actividades que lleva a cabo, los servicios que presta, los mercados de referencia, las funciones que desempeña y las expectativas de las autoridades y otras partes interesadas.
El cumplimiento de las disposiciones legales aplicables constituye un requisito ineludible y prevalece sobre las normas voluntarias, las prácticas, las certificaciones y las disposiciones contractuales. La conformidad se evalúa de forma concreta en relación con cada una de las empresas del Grupo, la función desempeñada, las actividades y los servicios efectivamente prestados, las tecnologías utilizadas, los datos tratados, los clientes y los destinatarios de los servicios, así como las posibles medidas, lineamientos y prescripciones de las autoridades competentes.

- **Protección de datos personales:** Reglamento (UE) 2016/679 (RGPD), Decreto Legislativo n.º 196 del 30 de junio de 2003, modificado por el Decreto Legislativo n.º 101 del 10 de agosto de 2018, así como las disposiciones y lineamientos aplicables de la Autoridad de protección de datos personales y del EDPB;

- **Inteligencia artificial:** Reglamento (UE) 2024/1689 (AI Act), en su versión vigente y de acuerdo con los plazos de aplicación correspondientes, incluidas las prohibiciones, las obligaciones en materia de formación y competencia, la clasificación de riesgos, la transparencia, la documentación, la supervisión humana, el seguimiento y la gestión de incidentes aplicables en función de la función que desempeñe el Grupo;
- **Ciberseguridad y resiliencia digital:** Directiva (UE) 2022/2555 (NIS2), tal y como ha sido transpuesta por el Decreto Legislativo n.º 138 del 4 de septiembre de 2024, siempre que el Grupo o las sociedades individuales entren dentro del ámbito de aplicación correspondiente o participen como proveedores o agentes de la cadena de suministro, además de los actos de aplicación y las resoluciones de la autoridad nacional competente en materia de redes de infraestructura estratégica (NIS);
- **Servicios digitales, documentos electrónicos y conservación:** Decreto Legislativo n.º 82 del 7 de marzo de 2005 (Código de la Administración Digital), Reglamento (UE) n.º 910/2014 (eIDAS), en su versión modificada, D.P.R. n.º 445 del 28 de diciembre de 2000 Directrices de la AgID sobre la creación, gestión y conservación de documentos electrónicos y otras normas técnicas aplicables;
- **Responsabilidad de la entidad, integridad y denuncias:** Decreto Legislativo n.º 231 del 8 de junio de 2001 y el Decreto Legislativo n.º 24 del 10 de marzo de 2023 en materia de denuncia de irregularidades, además de la normativa anticorrupción y de transparencia aplicable en las relaciones con las administraciones públicas;
- **Salud, seguridad, trabajo, medio ambiente e igualdad de oportunidades:** Decreto Legislativo n.º 81 del 9 de abril de 2008, Decreto Legislativo n.º 152 del 3 de abril de 2006, normativa laboral y convenios colectivos aplicables, Decreto Legislativo n.º 198 del 11 de abril de 2006, y demás disposiciones imperativas pertinentes;
- **Contratación pública, servicios a la Administración Pública y accesibilidad:** Decreto Legislativo n.º 36 del 31 de marzo de 2023, Ley n.º 4 del 9 de enero de 2004, y los requisitos técnicos correspondientes, en la medida en que sean aplicables a los suministros, servicios, plataformas e interfaces digitales creados o gestionados por el Grupo;
- **Actividad principal y seguridad vial:** Decreto Legislativo n.º 285 del 30 de abril de 1992 (Código de Circulación), D.P.R. n.º 495 del 16 de diciembre de 1992, normativa sobre los dispositivos y sistemas utilizados para la detección de infracciones, las correspondientes disposiciones de homologación o aprobación y las prescripciones de las autoridades competentes, en la medida en que sean pertinentes para los servicios y soluciones prestados;
- **Otros requisitos aplicables:** normativa europea, nacional, regional y local; autorizaciones, concesiones, prescripciones administrativas, obligaciones contractuales legítimas y requisitos sectoriales pertinentes a cada una de las actividades, sedes, infraestructuras, productos y servicios del Grupo.

Los modelos adoptados por Safety21 sitúan al cliente como prioridad: comprender plenamente sus necesidades y diseñar soluciones personalizadas garantizan el alcance de objetivos de excelencia. Para ello, la Dirección tomó la decisión estratégica de prestar la máxima atención a las necesidades de sus clientes, mejorando la comprensión de las mismas y supervisando constantemente el servicio y los procesos internos, con el fin de mantener unos niveles de rendimiento, disponibilidad y calidad acordes con los objetivos de la empresa.

El compromiso de la Dirección se materializa en un modelo integrado de gobernanza, gestión de riesgos y control de la conformidad, respaldado, cuando procede, por los sistemas de gestión certificados y las normas voluntarias adoptadas por el Grupo:

UNI EN ISO 9001 – Sistemas de gestión de calidad
ISO/IEC 27001 – Sistemas de gestión de la seguridad de la información

UNI CEI ISO/IEC 20000-1 – Requisitos de los sistemas de gestión de servicios
UNI EN ISO 14001 – Sistemas de gestión medioambiental
ISO/IEC 27017 – Tecnologías de la información
ISO/IEC 27018 - Tecnologías de la información
ISO/IEC 27701 – Sistemas de gestión de información de privacidad (RGPD)
ISO 22301 – Sistemas de gestión de la continuidad operativa
ISO 37001 – Sistemas de gestión anticorrupción
ISO 45001 – Sistemas de gestión de seguridad y salud en el trabajo
ISO 18295-1 – Centros de contacto con el cliente
UNI PDR 125 – Igualdad de género
SA 8000 – Sistemas de gestión de la responsabilidad social
Sistema de conservación conforme a la normativa (SdC)
Certificación B Corp

Además, la Dirección establece que las políticas y procedimientos de la empresa deberán ajustarse a:

- ✓ Los requisitos de las normas ISO conforme a las cuales está certificada, así como los requisitos de las normas SA8000 y PdR125;
- ✓ Las convenciones, recomendaciones y al Código de conducta sobre el VIH y el mundo del trabajo de la Organización Internacional del Trabajo (OIT);
- ✓ La Declaración universal de los derechos humanos;
- ✓ Las convenciones sobre los derechos del niño, la eliminación de la discriminación contra la mujer y la discriminación racial, así como los Principios rectores sobre las empresas y los derechos humanos de las Naciones Unidas (ONU);
- ✓ Los pactos internacionales sobre los derechos económicos, sociales, culturales, civiles y políticos;
- ✓ La legislación nacional aplicable, la normativa sectorial, las condiciones contractuales y cualquier otro requisito que se haya aceptado voluntariamente.

3. VALORES

Safety21 basa su actividad en valores sólidos y compartidos, que guían todos los aspectos de su funcionamiento y su cultura empresarial. Estos valores forman parte del Código Ético de Safety21 y se plasman en su compromiso con la responsabilidad social, la ética y la sostenibilidad.

El Grupo garantiza la coordinación entre las áreas competentes en materia de conformidad, protección de datos personales, seguridad de la información, ciberseguridad, inteligencia artificial, continuidad operativa, asuntos jurídicos, gestión de proveedores y control interno. Para cada ámbito se definen las funciones, las responsabilidades, las personas de contacto, los procesos de consulta y los criterios de escalamiento, con el propósito de evitar superposiciones y garantizando la participación oportuna de las áreas implicadas en los procesos de toma de decisiones y de planificación.

Safety21, como empresa certificada B Corp, reafirma su compromiso de generar un impacto positivo en las personas, las comunidades y el medio ambiente, integrando los principios de sostenibilidad y responsabilidad social en sus estrategias y actividades diarias.

La certificación B Corp reconoce los esfuerzos realizados por la empresa para conciliar el beneficio económico con el valor compartido, garantizando que los valores éticos mencionados anteriormente se traduzcan en acciones concretas y cuantificables, orientadas a la mejora continua y a la creación de beneficios duraderos para todas las partes interesadas.

- ✓ Ética del respeto: Safety21 reconoce la dignidad de cada persona y escucha activamente, valora las diferencias y actúa con integridad y transparencia. Fomenta la confianza mutua, reduce los conflictos y crea las condiciones necesarias para una colaboración auténtica y duradera;

- ✓ El valor de la persona y el reconocimiento del mérito: Safety21 cree en una cultura basada en el reconocimiento del valor y la confianza. La organización invierte en el desarrollo de su personal, escucha sus necesidades y fomenta su participación. Además, premia el esfuerzo, las competencias y los resultados obtenidos, motivando a las personas a dar lo mejor de sí mismas;
- ✓ Orientación al cliente: Safety21 depende de sus clientes y, por ello, se esfuerza por satisfacer sus necesidades actuales y futuras, cumplir con sus requisitos y superar sus propias expectativas.
- ✓ Coherencia entre valores, estrategias y comportamientos: Safety21 se compromete a garantizar que sus estrategias empresariales estén alineadas con los valores éticos declarados y que cada acción y decisión sea coherente con los principios éticos y profesionales de la empresa.
- ✓ Integridad, transparencia y legalidad en las relaciones con los proveedores y las partes interesadas: La empresa se compromete a basar sus relaciones con los proveedores, socios y demás partes interesadas en los principios de integridad, honestidad y respeto mutuo, garantizando prácticas comerciales éticas y conformes a la ley.
- ✓ Promoción de la defensa de los derechos humanos: La empresa defiende activamente los derechos humanos, comprometiéndose a respetarlos y promoverlos tanto dentro como fuera de la organización, contribuyendo así a una sociedad más justa y equitativa.
- ✓ Transparencia y diálogo con las instituciones: Safety21 fomenta una comunicación abierta y transparente con las instituciones, promoviendo el diálogo constructivo y la colaboración para mejorar las políticas públicas y de gobernanza.
- ✓ Salud y seguridad en el trabajo: La empresa presta especial atención a la creación de entornos de trabajo seguros y saludables, mediante la aplicación de medidas preventivas y de formación para proteger la salud y garantizar la seguridad de sus empleados.

4. CALIDAD Y PUNTOS DE CONTACTO PARA EL CLIENTE (UNI EN ISO 9001:2015, UNI EN ISO 18295-1:2017):
Safety21 se compromete a:

- ✓ Prestar servicios de alta calidad que satisfagan las necesidades y expectativas de los clientes:
  - CENTRÁNDONOS EN EL CLIENTE Y EN LAS PARTES INTERESADAS: Safety21 se compromete a comprender las necesidades de sus clientes y a planificar sus actividades para satisfacerlas plenamente. Del mismo modo, la Organización realiza sus actividades respetando las exigencias y los requisitos del mercado de referencia, del país en el que opera y de todas las partes implicadas en los procesos que considera críticos,así como cumpliendo con las leyes y reglamentos;
  - UTILIZANDO UN ENFOQUE A PROCESOS: Safety21 considera las distintas actividades de su organización como procesos que deben planificarse, controlarse y mejorarse continuamente, y optimiza el uso de los recursos necesarios para llevarlas a cabo. Además, gestiona sus propios procesos de manera que los objetivos, los resultados esperados, las responsabilidades asociadas y los recursos empleados sean inequívocos.
  - DEMOSTRANDO SU LIDERAZGO: Safety21 asume la responsabilidad del correcto funcionamiento de su SGI, poniendo a disposición todos los recursos necesarios y garantizando que los objetivos establecidos sean compatibles con el contexto y las directrices estratégicas.
  - IDENTIFICANDO RIESGOS Y OPORTUNIDADES: Safety21 planifica sus procesos aplicando un pensamiento basado en riesgos (RBT) con el fin de implementar las acciones más adecuadas para evaluar y tratar los riesgos asociados a los procesos, así como para aprovechar y reforzar las oportunidades identificadas.

- ✓ Aumentar constantemente la satisfacción de los clientes, prestando atención tanto a los requisitos explícitos (aquellos que figuran expresamente en los contratos de suministro) como a los implícitos;

- ✓ Lograr un crecimiento adecuado del nuevo negocio;
- ✓ Garantizar la continuidad operativa y minimizar el impacto en el negocio en caso de crisis, asegurando un rápido regreso a la normalidad de las actividades empresariales;
- ✓ Proteger los intereses de Safety21 y aumentar la confianza de sus clientes y socios, prestando especial atención a los niveles de servicio mediante el desarrollo y la implementación de mecanismos que garanticen la continuidad del servicio prestado, de conformidad con los SLA definidos;
- ✓ Supervisar los procesos empresariales con herramientas adecuadas de seguimiento y control;
- ✓ Trabajar para lograr la participación del personal y el desarrollo de sus competencias mediante la organización de sesiones de formación e información, con el fin de fomentar el crecimiento, la concienciación y el sentido de la responsabilidad de toda la plantilla, así como garantizar un alto nivel de profesionalidad del personal, tanto a nivel directivo y de gestión como operativo;
- ✓ Garantizar que el intercambio de información y la sinergia entre las áreas constituyan valores estratégicos;

Los socios comerciales se clasifican en categorías de riesgo (bajo, medio, alto) según los criterios objetivos establecidos en el Análisis de Riesgos de la norma ISO 37001.
Las principales categorías son:

- ✓ Proveedores y asesores operativos: riesgo *medio*, deben someterse a una auditoría de debida diligencia anual;
- ✓ Socios en consorcios, RTI, ATI y empresas conjuntas: riesgo *alto*, debida diligencia previa y reevaluación anual;
- ✓ Intermediarios, agentes y socios comerciales extranjeros: riesgo *alto*, verificación de los beneficiarios efectivos y comprobación externa de la reputación;
- ✓ Beneficiarios de subvenciones y patrocinios: riesgo *medio-alto*, verificación previa de las fuentes de financiación.

5. SALUD Y SEGURIDAD EN EL TRABAJO (UNI EN ISO 45001:2023)

El objetivo principal de Safety21 es proteger la salud y la seguridad de sus empleados y colaboradores y, por ello, se compromete a minimizar los riesgos y a mejorar su desempeño en materia medioambiental y de seguridad.

Safety21 se compromete a:

- ✓ Proporcionar un entorno de trabajo seguro y saludable;
- ✓ Garantizar el cumplimiento de la normativa aplicable (Decreto Legislativo n.º 81/2008 y sus respectivas modificaciones y adiciones) y de las normas en materia de salud y seguridad en el trabajo, así como un entorno laboral saludable, seguro y cómodo para toda la plantilla;
- ✓ Identificar y mitigar los riesgos para la salud y la seguridad mediante evaluaciones periódicas y mejoras continuas;
- ✓ Fomentar una cultura de la seguridad mediante la formación y la sensibilización;
- ✓ Prevenir accidentes y daños a la salud de los trabajadores, comprometiéndose a mejorar continuamente las medidas de seguridad y de salud en los lugares de trabajo;
- ✓ Reducir al mínimo los riesgos para la salud y la seguridad de los trabajadores mediante la adopción de medidas adecuadas de evaluación y protección, aplicables en función de las actividades realizadas;
- ✓ Elevar progresivamente los «estándares» de calidad y salud mediante programas de mejora y sistemas de gestión y control que permitan llevar a cabo una evaluación adecuada de los riesgos y adoptar medidas correctivas;
- ✓ Facilitar al personal la información necesaria sobre los riesgos a los que puedan estar expuestos con las actividades que realizan;

- ✓ Involucrar y consultar a los responsables en materia de seguridad laboral y seguridad informática;
- ✓ Seguimiento de las solicitudes del personal, de los clientes y de las asociaciones (sociales, sindicales, políticas, etc.), teniendo en cuenta su sensibilidad y expectativas en materia de protección de la salud, seguridad y medio ambiente, con el fin de garantizar una relación de transparencia y colaboración con el tejido social;
- ✓ Sensibilización de los proveedores para que adopten procedimientos destinados a garantizar el cumplimiento de la normativa y mejoren progresivamente los niveles de salud y seguridad en el trabajo.

6. MEDIO AMBIENTE (UNI EN ISO 14001:2015) – B Corp

El objetivo principal de Safety21 es proteger el medio ambiente y, por ello, se compromete a minimizar el impacto medioambiental y a mejorar su desempeño medioambiental.
Safety21 se compromete a:

- ✓ Reducir el impacto medioambiental de sus actividades mediante prácticas sostenibles, como el ahorro energético y el uso eficiente de los recursos;
- ✓ Fomentar el reciclaje y la gestión responsable de los residuos.
- ✓ Supervisar y mejorar continuamente el desempeño medioambiental, de conformidad con las leyes y normativas medioambientales relacionadas con sus actividades;
- ✓ Llevar a cabo una gestión consciente y sostenible de los recursos naturales y de la energía, optimizando su uso y reduciendo el desperdicio;
- ✓ Responsabilizar y sensibilizar al personal implicado en las actividades de la empresa en todos los niveles, mediante programas adecuados de información y formación, para que todo el personal garantice la implementación y aplicación efectiva del Sistema de Gestión Medioambiental en el ámbito de sus competencias;
- ✓ Velar por el cumplimiento de lo establecido en las autorizaciones medioambientales otorgadas a la empresa;
- ✓ Analizar sistemáticamente el Sistema de Gestión Medioambiental con el objetivo de mejorar continuamente su desempeño.
- ✓ Garantizar que toda la plantilla participe, en función de sus atribuciones y competencias, en la consecución de los objetivos asignados;
- ✓ Elaborar un análisis de riesgos que permita conocer y evaluar el nivel de exposición al riesgo de su propio sistema de gestión. En función de ese nivel, determinar las medidas de seguridad adecuadas;
- ✓ Garantizar la revisión de la política de la empresa (al menos una vez al año), teniendo en cuenta los posibles cambios legislativos y cualquier otro requisito de la empresa;
- ✓ Que sus actividades y negocios se lleven a cabo a fin de evitar la implicación en cualquier caso de corrupción u otras actividades ilícitas;
- ✓ Integrar los principios de sostenibilidad en todos los procesos de la empresa, promoviendo el uso de tecnologías limpias y renovables;
- ✓ Apoyar las iniciativas de desarrollo sostenible y colaborar con las partes interesadas para promover prácticas sostenibles;
- ✓ Garantizar la transparencia y la responsabilidad en las actividades de la empresa.

7. CIBERSEGURIDAD, RESILIENCIA DIGITAL Y GESTIÓN DE SERVICIOS

(DIRECTIVA UE 2022/2555, DECRETO LEGISLATIVO 138/2024 Y NORMAS APLICABLES)

Safety21 reconoce que la seguridad de la información, la resiliencia cibernética, la protección de los datos personales y el uso responsable de las tecnologías digitales y de la inteligencia artificial son factores estratégicos para la continuidad operativa, la confianza de las partes interesadas y la creación de valor sostenible.

Los órganos de administración y la Dirección definen y aprueban las directrices estratégicas para la gestión de los riesgos de ciberseguridad, supervisan su aplicación y reciben informes periódicos sobre la exposición a los riesgos, el estado de las medidas, los incidentes significativos, las vulnerabilidades relevantes y los planes de mejora. La ejecución operativa recae en los órganos competentes, de acuerdo con las funciones, las facultades delegadas y las responsabilidades definidas formalmente.

La gestión de la ciberseguridad y de los sistemas de inteligencia artificial se lleva a cabo, en función del ámbito de aplicación efectivo y de la función que desempeña el Grupo, de conformidad con el Decreto Legislativo n.º 138 del 4 de septiembre de 2024, por el que se incorpora la Directiva (UE) 2022/2555 (NIS2), el Reglamento (UE) 2024/1689 (AI Act), los actos de aplicación y las prescripciones de las autoridades competentes. El Grupo verifica y documenta periódicamente su ámbito de aplicación, también en lo que respecta a las sociedades controladas, a los servicios prestados, a la cadena de suministro y a los sistemas de IA desarrollados, suministrados, importados, distribuidos o utilizados.

Safety21 se compromete, a nivel de grupo, a garantizar y promover un enfoque estructurado de la gestión de los riesgos cibernéticos, asegurando la identificación, la evaluación, el tratamiento y el seguimiento continuo de las amenazas informáticas que puedan comprometer la confidencialidad, la integridad y la disponibilidad de la información y de los servicios prestados;

- ✓ Reforzar la resiliencia digital de la organización mediante la adopción de medidas técnicas y organizativas adecuadas para la prevención, detección, gestión y respuesta ante incidentes de seguridad informática, de conformidad con los principios de la Directiva NIS2 y la normativa aplicable;

El Grupo aplica un proceso estructurado de gestión de incidentes que regula la identificación, la clasificación, la contención, la respuesta, la recuperación, la recopilación de pruebas, las comunicaciones internas y externas y el análisis de las causas. Cuando proceda, el proceso garantiza el cumplimiento de los plazos y los contenidos previstos para las notificaciones a las autoridades competentes, así como la coordinación con las obligaciones contractuales, de protección de datos, de continuidad operativa y de información a los clientes y a las partes interesadas.

- ✓ Garantizar la supervisión continua de la exposición a los riesgos cibernéticos, fomentando las actividades de gestión de vulnerabilidades, la gestión de las actualizaciones de seguridad, la protección de las infraestructuras críticas y la verificación de la eficacia de los controles implementados;
- ✓ Garantizar una gestión segura de la cadena de suministro de las TIC mediante criterios establecidos para la cualificación, selección, contratación, seguimiento y revisión de los proveedores y socios que participan en la prestación de servicios digitales y en la nube. La evaluación tiene en cuenta, como mínimo, el nivel de criticidad de los servicios, el acceso a datos y sistemas, las dependencias operativas, la continuidad, la ubicación y la cadena de subcontratistas, las obligaciones en materia de seguridad y notificación de incidentes, así como las modalidades de devolución o supresión de la información al término de la relación.
- ✓ Garantizar que el uso de tecnologías innovadoras, incluidas las soluciones basadas en la inteligencia artificial, cuente con autorización previa y se lleve a cabo respetando los requisitos aplicables en materia de seguridad, fiabilidad, transparencia, protección de datos, defensa de los derechos fundamentales y supervisión humana. El Grupo identifica la función que desempeña en relación con cada sistema, documenta su finalidad y su nivel de riesgo, verifica a los proveedores y supervisa a lo largo del tiempo el rendimiento, las anomalías, los incidentes y las repercusiones sobre los interesados y el resto de partes interesadas.
- ✓ Fomentar un nivel adecuado de competencia y concienciación entre el personal que desarrolla, adquiere, configura, utiliza o supervisa sistemas de inteligencia artificial, mediante programas de formación adaptados a las funciones, los contextos de uso y los riesgos asociados. La formación también abarca los límites de uso de las herramientas, la calidad y la confidencialidad de los datos introducidos, la verificación de los resultados, la supervisión humana y los procedimientos para

notificar anomalías o incidentes. Garantizar que existan mecanismos adecuados de identificación, autenticación y autorización, de modo que solo las personas autorizadas puedan acceder a la información y a los recursos de la empresa.

- ✓ Garantizar que los aspectos relacionados con la seguridad y la protección de los datos personales se tengan en cuenta en todas las fases de diseño, desarrollo, funcionamiento, mantenimiento, asistencia y retirada de los sistemas y servicios informáticos;
- ✓ Garantizar la continuidad de la actividad de Safety21 y el eventual restablecimiento de los servicios que se vean afectados por incidentes de cierta gravedad, reduciendo las consecuencias tanto dentro como fuera del ámbito empresarial;
- ✓ Que las normas de seguridad se mantengan y supervisen de acuerdo a lo señalado por la certificación ISO 27001;
- ✓ Vigilar e identificar las vulnerabilidades del sistema de información, supervisando las posibles fallas de las aplicaciones y del hardware utilizados;
- ✓ Definir, aplicar y supervisar los objetivos relativos a los planes de gestión del servicio, de continuidad, de disponibilidad, de capacidad y de puesta en marcha, tal y como establece la norma de referencia;
- ✓ Definir, mantener y mejorar el catálogo de servicios de acuerdo con las necesidades de sus clientes, diseñando y prestando servicios, incluso innovadores, que les aporten un aumento de valor;
- ✓ Apoyar a la dirección y a todo el personal para que alcancen un nivel de conocimiento, concienciación y habilidades que permita reducir al mínimo los riesgos de posibles daños derivados de incidentes que afecten a la seguridad de la información;

8. 8. PROTECCIÓN DE DATOS PERSONALES Y GOBERNANZA DE LA INFORMACIÓN

(REGLAMENTO (UE) 2016/679, NORMATIVA NACIONAL APLICABLE E ISO/IEC 27701)

El Grupo regula la protección de los datos personales y de la información mediante un modelo organizativo integrado, adaptado a las actividades de cada una de las sociedades, a los servicios efectivamente prestados y a las funciones desempeñadas en los distintos tratamientos. El modelo garantiza el cumplimiento del Reglamento (UE) 2016/679 y del Decreto Legislativo n.º 196 del 30 de junio de 2003, y de las demás disposiciones, requisitos y directrices aplicables, coordinando las obligaciones en materia de protección de datos con las relativas a la ciberseguridad, la inteligencia artificial, los servicios a la Administración Pública, la detección de infracciones, la gestión documental y la conservación.

Los órganos de administración y la Dirección establecen las directrices y garantizan los recursos adecuados; cada sociedad del Grupo asume las responsabilidades propias de su función y de su ámbito operativo. Para cada tratamiento, servicio o proyecto se identifican y documentan el responsable o los posibles corresponsables, los encargados y los subencargados, las personas autorizadas, el responsable del proceso y las áreas que deben participar en la toma de decisiones. El Área de privacidad coordina las medidas operativas y la actualización de la documentación; el DPO desempeña de forma autónoma las funciones de asesoramiento, supervisión y diálogo previstas en la normativa, sin asumir responsabilidades decisorias u operativas incompatibles con su cargo.

- ✓ definir, mediante matrices RACI, delegación de competencias, poderes y procedimientos, responsabilidades, facultades de decisión, obligaciones de consulta y flujos de escalamiento entre el Área de privacidad, el DPO, el Departamento Jurídico y de Cumplimiento, Ciberseguridad/TIC, Gobernanza de la IA, Adquisiciones, Recursos Humanos, los responsables de función y los propietarios de procesos;
- ✓ mantener un catálogo actualizado de los tratamientos, los servicios, los sistemas, las bases de datos y sus respectivos responsables, coordinado con los registros de las actividades de tratamiento, el inventario de activos, el censo de los sistemas de inteligencia artificial y la documentación contractual;

- ✓ aplicar un proceso preventivo y documentado de evaluación de los nuevos proyectos, productos, servicios, proveedores y cambios relevantes, garantizando la privacidad y la seguridad desde el diseño y por defecto y, cuando sea necesario, realizando evaluaciones de impacto, análisis de riesgos, consultas al DPO y obteniendo la autorización de las áreas competentes;
- ✓ regular las relaciones intragrupo y con terceros de acuerdo con las funciones efectivamente asumidas, verificando las instrucciones, las medidas de seguridad, la subcontratación, las transferencias internacionales, los plazos de conservación, la devolución o supresión de los datos y las obligaciones de asistencia y notificación;
- ✓ garantizar que las decisiones que afecten a los datos personales sean adoptadas por la persona competente, sean trazables y tengan en cuenta las indicaciones de las áreas de control, previendo su escalamiento a la Dirección o a los órganos sociales competentes en caso de riesgos inaceptables, divergencias significativas o cuestiones que requieran una decisión estratégica.

El modelo de responsabilidad proactiva incluye la definición de las bases jurídicas y las finalidades, la minimización de los datos, la calidad y exactitud de la información, la gestión de los derechos de los interesados, la determinación y la revisión de los plazos de conservación, la formación de las personas autorizadas y el seguimiento de la eficacia de los controles. Las violaciones de datos personales se gestionan mediante un proceso coordinado con la gestión de incidentes cibernéticos y operativos, lo que garantiza la intervención oportuna de los departamentos de Privacidad, del DPO, del departamento Jurídico, de Ciberseguridad/TIC, de los responsables de procesos, de Comunicación y de la Dirección, así como las evaluaciones, notificaciones, comunicaciones y medidas correctivas que puedan ser necesarias.

- ✓ proteger los datos personales y la información a lo largo de todo su ciclo de vida mediante medidas técnicas y organizativas adecuadas, integradas en los sistemas de gestión de la seguridad de la información, la continuidad operativa y los servicios;
- ✓ establecer indicadores, controles periódicos y flujos de información hacia la Dirección y los órganos competentes, incluyendo riesgos, incidentes, solicitudes de los interesados, estado de las evaluaciones de impacto, proveedores críticos, transferencias, conservación, formación, incumplimientos y planes de mejora;
- ✓ someter el modelo a revisión con motivo de cambios normativos, organizativos o tecnológicos, la introducción de nuevos servicios o sistemas de inteligencia artificial, de modificaciones en las funciones relacionadas con la protección de datos, de operaciones societarias, de incidentes significativos o de los resultados de auditorías y verificaciones;
- ✓ promover competencias específicas según el puesto de trabajo y una cultura común en materia de protección de datos e información, de modo que el personal, los colaboradores y los terceros actúen conforme a las instrucciones, responsabilidades y límites de uso claramente definidos.

9. IGUALDAD DE GÉNERO (UNI PDR 125:2022) – B Corp

Safety21 cree en una cultura basada en el respeto y la valorización de la diversidad de género, edad, origen, condición social, religión, ideas políticas, capacidades físicas y mentales, identidad y orientación sexual.

Safety21 se compromete a:

- ✓ Mejorar el entorno laboral fomentando y apoyando la inclusión, la igualdad de género y el reconocimiento de la diversidad de género.
- ✓ Aplicar un modelo de gobernanza de la organización destinado a definir los mecanismos organizativos adecuados y garantizar la presencia del género minoritario en los órganos de dirección y control de la organización, así como la existencia de procesos destinados a identificar y corregir cualquier caso de exclusión;

- ✓ Poner en marcha procesos en el ámbito de recursos humanos, relacionados con las distintas etapas que caracterizan el ciclo de vida de un empleado en la organización, basados en los principios de inclusión y respeto a la diversidad;
- ✓ Fomentar un entorno laboral inclusivo y libre de discriminación de género;
- ✓ Garantizar la igualdad de oportunidades profesionales y de desarrollo profesional para todos los empleados;
- ✓ Promover y valorar la maternidad y la paternidad mediante la aplicación de políticas de conciliación de la vida laboral y familiar y apoyar el equilibrio entre las responsabilidades profesionales y personales;
- ✓ Crear oportunidades de diálogo continuas y adecuadas para mantener un entorno inclusivo mediante encuestas de opinión periódicas y campañas de sensibilización sobre cuestiones de igualdad de género en las que participe toda la plantilla, con el fin de comprender sus percepciones y necesidades, y permitir que los empleados aporten ideas valiosas que sirvan para definir las iniciativas de la empresa;
- ✓ La eliminación de cualquier forma de intimidación, acoso y violencia;
- ✓ La aplicación de los principios de igualdad de oportunidades y meritocracia en la gestión de todas las fases del ciclo de vida del personal (desde la selección y la contratación hasta el acceso a la formación y las trayectorias de desarrollo, incluida la remuneración) garantiza todos los aspectos de la igualdad de género;
- ✓ Garantizar la igualdad de género en todas las funciones y puestos, y en todos los niveles de la jerarquía:
- ✓ Fomentar un proceso de selección basado en criterios inclusivos que contemple un análisis de los datos de selección que permita realizar un seguimiento de la composición de la plantilla de la empresa en términos de género;
- ✓ Ofrecer programas de formación que ayuden a comprender y reconocer los prejuicios inconscientes, centrados en el trabajo en equipo inclusivo y en ofrecer una experiencia al cliente basada en el valor de la inclusión;
- ✓ Ofrecer programas de formación dirigidos a directivos, con el objetivo de potenciar y reforzar un liderazgo inclusivo;
- ✓ Fomentar el desarrollo de las competencias de las mujeres a través de programas específicos, como sesiones de tutoría, coaching y formación en liderazgo, para ayudar a las mujeres con talento a acceder a puestos directivos;
- ✓ Apoyar al Comité Directivo encargado de supervisar el Sistema de gestión de la igualdad de género en las actividades destinadas a eliminar la discriminación y cualquier obstáculo que, de hecho, impida la igualdad entre hombres y mujeres en el acceso al empleo, en la promoción y en la formación profesional, así como en las condiciones de trabajo, incluida la remuneración;
- ✓ Que el empoderamiento de las mujeres sea una prioridad: Las mujeres deben estar bien representadas en todos los niveles, así como en los paneles de mesas redondas, congresos y demás eventos organizados tanto dentro como fuera de la empresa.

10. ANTICORRUPCIÓN (UNI ISO 37001:2025)

La Organización adopta un enfoque ético, transparente y conforme a la normativa en todos los ámbitos de su actividad, y reconoce la prevención del soborno como un compromiso fundamental con sus partes interesadas, tanto públicas como privadas. La Organización ha creado una Función para la prevención del soborno, dotada de autonomía, independencia y recursos adecuados, cuya misión es velar por la aplicación efectiva del sistema de prevención, promover la cultura de la integridad y garantizar el seguimiento constante del cumplimiento de las normas internas y externas en materia de anticorrupción.

Safety21 se compromete a:

- ✓ Prohibir el soborno en todas sus formas;

- ✓ Desarrollar, mantener y difundir una sólida cultura antisoborno en todos los niveles de la organización, promoviendo valores que fomenten el rechazo de las prácticas ilícitas y el respeto a la legalidad;
- ✓ Crear un entorno desfavorable para el soborno, aumentando la capacidad para detectar casos de soborno y fomentando la transparencia de la actividad y de la organización;
- ✓ Evaluar periódicamente los riesgos de soborno, teniendo en cuenta la evolución del contexto externo, incluidos los factores relacionados con el cambio climático cuando sean relevantes para las actividades del Grupo;
- ✓ Fomentar la denuncia de posibles casos de soborno, de buena fe, o sobre la base de una creencia razonable y confidencial, garantizando la protección frente a represalias, discriminación o medidas disciplinarias de quienes denuncien o se nieguen a participar en actos de soborno;
- ✓ Mantener activo y mejorar de forma continua el Sistema de gestión anticorrupción de conformidad con la norma ISO 37001:2025, asegurando que la diligencia debida en relación a los socios comerciales se lleve a cabo en la fase preventiva y que se actualice mediante un seguimiento continuo en función del nivel de riesgo;
- ✓ Garantizar un nivel adecuado de formación e información para todo el personal y los socios comerciales mediante actividades periódicas de divulgación, resúmenes informativos y herramientas de comunicación, con el fin de mejorar el Sistema de gestión anticorrupción;
- ✓ Garantizar que el Sistema de gestión anticorrupción cumpla con la norma UNI ISO 37001:2025, mediante la realización periódica de auditorías internas, en virtud de la autoridad y la independencia que se le han conferido;
- ✓ Garantizar la eficacia, eficiencia y fiabilidad, utilizando todos los recursos necesarios para asegurar el cumplimiento de los principios de diligencia, transparencia y corrección;
- ✓ Identificar y gestionar de forma proactiva los conflictos de intereses, reales o potenciales, que pudieran facilitar prácticas corruptas;
- ✓ Iniciar las medidas disciplinarias o legales oportunas contra aquellas personas que hayan tenido un comportamiento ilícito contrario a los principios de la presente política;
- ✓ Garantizar la autoridad y la independencia de la Función anticorrupción.

Safety21 considera la denuncia un instrumento eficaz para combatir el soborno y fomenta la denuncia de presuntos casos de soborno, incluso de forma anónima.

Los canales de notificación son los siguientes:

- ✓ Aplicación para la denuncia de irregularidades que permite enviar notificaciones o reclamaciones, incluso de forma anónima, publicada en la página web de la empresa en el siguiente enlace https://safety21.integrityline.com/.
- ✓ Correo electrónico del Organismo de Vigilancia: odv@safety21.it – odv@gefilspa.it – odv@spv21ventimiglia.it.
- ✓ Correo postal en sobre cerrado a la siguiente dirección: Safety21 S.A. - a la atención del Órgano de Vigilancia —Via Lepetit, 8 – 20124 Milán—, indicando la mención «Confidencial: personal».

11. CONTINUIDAD OPERATIVA (ISO 22301:2019)

Safety21 reconoce la importancia estratégica de la continuidad operativa para garantizar la resiliencia de sus servicios, la protección de las partes interesadas y el cumplimiento de las obligaciones contractuales y normativas. De acuerdo con los requisitos de la norma ISO 22301:2019, la organización se compromete a:

- ✓ Garantizar la disponibilidad de los recursos necesarios para restablecer los procesos y servicios esenciales dentro de los plazos establecidos, minimizando el impacto para los clientes, los ciudadanos y los socios institucionales;

- ✓ Cumplir con las restricciones y los requisitos contractuales acordados y detallados en el Análisis de impacto empresarial realizado en el ámbito de aplicación del Sistema de gestión de la continuidad del negocio;
- ✓ Garantizar la protección de la vida humana ante una situación de crisis;
- ✓ Garantizar, en caso de crisis, la continuidad operativa minimizando el impacto en la actividad de la organización;
- ✓ Garantizar la implementación de una arquitectura resiliente;
- ✓ Proteger los intereses de la organización y de las partes interesadas relevantes, prestando la máxima atención a los aspectos relacionados con la disponibilidad, el cumplimiento de los niveles de servicio y la conformidad con la normativa vigente y los compromisos contractuales.

12. SISTEMA DE CONSERVACIÓN (SDC)

Safety21 considera que la gestión y conservación de los documentos electrónicos es un proceso estratégico para garantizar la transparencia, la trazabilidad y la protección del valor jurídico de la información tratada por cuenta de la Administración Pública. De acuerdo con lo establecido en el Código de administración digital (CAD), las Directrices de la AgID y la normativa vigente en materia de digitalización, la organización ha implementado un Sistema de conservación (SdC) conforme y seguro.
El Sistema de conservación se rige de conformidad con el Decreto Legislativo n.º 82 del 7 de marzo de 2005, al D.P.R. n.º 445 del 28 de diciembre de 2000, al Reglamento (UE) n.º 910/2014 (eIDAS), en su versión modificada, a las Directrices de la AgID sobre la creación, gestión y conservación de documentos electrónicos, y a los demás requisitos técnicos y sectoriales aplicables. Los plazos de conservación se establecen en función de las finalidades y las obligaciones legales pertinentes, y se ajustan a los principios de limitación de la conservación y minimización de los datos personales.

Safety21 se compromete a:

- ✓ Gestionar el ciclo de vida de los documentos de forma controlada, desde su creación hasta su conservación, de conformidad con los manuales de conservación, los planes de clasificación y los metadatos establecidos;
- ✓ la identificación fehaciente de la persona que ha elaborado el documento y de la administración o del área organizativa homogénea de referencia, es decir, la identificación de su procedencia para evaluar sus características de autenticidad;
- ✓ la integridad del documento;
- ✓ la legibilidad y la facilidad para localizar los documentos y la información identificativa, incluidos los datos originales de registro y clasificación, así como los metadatos asociados a los documentos, la definición de las agrupaciones documentales y las estructuras de archivo de referencia;
- ✓ Llevar a cabo un seguimiento, auditorías y actualizaciones continuas del sistema, también en relación con la evolución normativa y tecnológica;
- ✓ Proteger los datos y los documentos mediante infraestructuras tecnológicas seguras y fiables, garantizando la seguridad lógica, física y organizativa del sistema.

13. RESPONSABILIDAD SOCIAL (SA8000) – B Corp

Ser un socio de confianza para las administraciones públicas y las fuerzas policiales implica contar, dentro de la propia plantilla, con personal que posea competencias transversales y multidisciplinares en el ámbito tecnológico y de la seguridad vial. Safety21 es consciente, por tanto, de sus responsabilidades para con la comunidad y pretende establecer como objetivo estratégico el compromiso de actuar de acuerdo con los principios de la responsabilidad social.

La Dirección se compromete a:

- ✓ No utilizar ni apoyar ninguna forma de trabajo infantil, estableciendo en todo caso procedimientos correctivos ante la detección de posibles casos;
- ✓ No emplear ni recurrir al trabajo forzoso y/u obligatorio;
- ✓ Garantizar el cumplimiento de la normativa aplicable en materia de seguridad e higiene en el trabajo;

Promover todas las iniciativas sindicales presentadas por los trabajadores y fomentar la expresión de puntos de vista diferentes como contribución fundamental a la resolución de problemas, garantizando que la libertad de expresión, tanto dentro como fuera de la Organización, quede protegida frente a cualquier tipo de represalia;

- ✓ No discriminar por ningún motivo a los trabajadores a lo largo de toda su vida laboral (selección, contratación, remuneración, acceso a la formación, promoción y cese de la relación laboral);
- ✓ No utilizar métodos coercitivos, ya sean físicos (como los castigos corporales) o psicológicos (como los abusos verbales o el acoso laboral) hacia los trabajadores;
- ✓ Respetar en todo momento la legislación vigente en materia laboral y aplicar correctamente los convenios colectivos nacionales del sector, también en lo que se refiere a la jornada laboral y a la carga de trabajo máxima, así como a las horas extraordinarias o al trabajo nocturno;
- ✓ Aplicar rigurosamente las tablas salariales previstas en los Convenios colectivos nacionales de trabajo del sector, según la categoría y el nivel, garantizando asimismo que los importes se abonen con regularidad y que sean suficientes para garantizar un nivel de vida digno (salario digno) al núcleo familiar del trabajador;
- ✓ Mantener a lo largo del tiempo los requisitos del sistema, verificando periódicamente su eficacia y garantizando un esfuerzo constante hacia la mejora continua de la gestión, mediante la definición de objetivos alcanzables y el seguimiento de su consecución.

La eficacia del modelo se verifica mediante indicadores, controles periódicos, auditorías, gestión de los incumplimientos, seguimiento de los planes de gestión de riesgos y presentación de informes a los órganos competentes. Los resultados de las verificaciones sirven de base para la revisión por parte de la Dirección, la actualización de las prioridades y los recursos, las medidas correctivas y los programas de mejora, garantizando la trazabilidad de las decisiones y las responsabilidades.

14. COMUNICACIÓN Y DIFUSIÓN

Safety21 considera que la comunicación interna y externa es un elemento esencial para la eficacia de sus sistemas de gestión. La Política Integrada se difunde de forma transparente, accesible y coherente, con el fin de que se comprenda, se acepte y se confirme su lectura.

En concreto, la organización se compromete a:

- ✓ Publicar la Política Integrada en la página web institucional de Safety21, poniéndola a disposición de clientes, socios, ciudadanos, proveedores y organismos públicos, como muestra de transparencia y responsabilidad.
- ✓ Publicar la política en la Intranet de la empresa, garantizando a todo el personal un acceso sencillo y continuo a los principios y compromisos de la empresa.
- ✓ Exponer la política en los lugares de trabajo, cuando proceda, para fomentar su visibilidad en los entornos operativos.
- ✓ Incorporar la política en los procesos de incorporación de los nuevos empleados, asegurándose de que comprendan los valores y las normas de la empresa desde el primer día de trabajo.
- ✓ Utilizar los canales de comunicación interna (boletines informativos, tablones de anuncios digitales, plataformas de RR. HH., reuniones periódicas) para mantener al personal al corriente y sensibilizarlo sobre cualquier cambio o iniciativa relacionada con la política.

15. ACTUALIZACIÓN Y REVISIÓN

Safety21 garantiza que su Política integrada se mantenga constantemente actualizada, vigente y adecuada a la evolución del contexto organizativo, normativo, tecnológico y estratégico.

La política se revisa al menos una vez al año, con motivo de la Revisión de la Dirección, y cada vez que se produzcan cambios significativos en el marco normativo, en la estructura societaria u organizativa, en las funciones que desempeña el Grupo, en los servicios y las tecnologías utilizadas, en el perímetro de la NIS, en el tratamiento de datos personales o en los sistemas de inteligencia artificial. Además, la revisión tiene en cuenta los incidentes, las violaciones de datos personales, las notificaciones, los incumplimientos, los resultados de las auditorías y los controles, las indicaciones de las autoridades, los cambios en la cadena de suministro y la evolución de los riesgos.

- ✓ Evolución del contexto externo o interno (por ejemplo, nuevos requisitos normativos, cambios estructurales, ampliación del ámbito de los servicios);
- ✓ Implementación o modificación de sistemas de gestión certificados;
- ✓ Acontecimientos significativos (accidentes, emergencias, incumplimientos graves, observaciones de auditoría);
- ✓ Cambios en los objetivos de la empresa o en las necesidades de las partes interesadas.

El responsable del Sistema de gestión integrado, en colaboración con las áreas competentes en la materia, coordina la propuesta de actualización de la política y verifica su coherencia con el marco normativo aplicable, con la estructura organizacional del Grupo y con la documentación interna relacionada. Quedan intactas las responsabilidades propias de los órganos de administración, la Dirección, el DPO, las áreas de control y los responsables operativos, de acuerdo con sus respectivas atribuciones y sin superposición de funciones.

La Dirección y, en sus respectivos ámbitos de competencia, los órganos de administración aprueban formalmente la Política, garantizan su integración en las directrices estratégicas del Grupo y verifican que se disponga de las responsabilidades, competencias y recursos adecuados para su aplicación. La aprobación no sustituye a los demás actos, acuerdos o documentos exigidos por la normativa aplicable.