					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P37S					Título del documento: **Política de Cumplimiento Legal y Normativo**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Control 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
RGPD de la UE	Artículos 5, 6, 32, 33	
Directiva NIS2 de la UE	Artículos 21(2)(a), 21(2)(f), 23	
DORA de la UE	Artículos 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Propósito

1.1 Esta política define el enfoque de la organización para identificar, cumplir y demostrar el cumplimiento de las obligaciones legales, reglamentarias y contractuales.

1.2 Establece responsabilidades claras y medidas prácticas para ayudar a la organización a cumplir sus obligaciones en materia de cumplimiento, incluidas las leyes de protección de datos, los marcos de ciberseguridad, los acuerdos con clientes y las normas de certificación.

1.3 Garantiza que, incluso sin un equipo de cumplimiento dedicado, la organización pueda mantener operaciones jurídicamente sólidas, responder adecuadamente a los incidentes y conservar una preparación completa para auditorías.

1.4 Esta política es esencial para posibilitar la certificación ISO/IEC 27001:2022 y satisfacer las expectativas externas de clientes, reguladores o socios.

2. Alcance

2.1 Esta política aplica a:

2.1.1 Todos los empleados, contratistas, autónomos y proveedores externos.

2.1.2 Todos los servicios, operaciones, sistemas y actividades de tratamiento de datos en los que la organización deba cumplir requisitos legales o contractuales.

2.1.3 Todas las ubicaciones y dispositivos utilizados para tratar información de la organización, ya sea en la oficina, en trabajo remoto o alojados en la nube.

2.2 La política cubre:

2.2.1 Leyes de protección de datos como el RGPD de la UE.

2.2.2 Reglamentos de ciberseguridad como la Directiva NIS2 de la UE.

2.2.3 Obligaciones específicas del sector, cuando proceda.

2.2.4 Contratos con clientes, acuerdos de confidencialidad y cláusulas de auditoría.

2.2.5 Certificaciones voluntarias (por ejemplo, ISO 27001) y políticas internas que deban aplicarse para garantizar el cumplimiento.

3. Objetivos

3.1 Establecer la responsabilidad proactiva: asignar una responsabilidad clara para supervisar, actualizar y hacer cumplir las obligaciones legales, reglamentarias y contractuales.

3.2 Proteger a la organización: minimizar el riesgo de incumplimientos legales, sanciones, violaciones de seguridad de los datos y daños reputacionales.

3.3 Facilitar la preparación para auditorías: mantener registros verificables que demuestren cómo la organización cumple sus obligaciones.

3.4 Respaldar la integración de políticas: garantizar que las obligaciones legales y reglamentarias se apliquen de forma coherente en todas las políticas y procesos.

3.5 Gestionar excepciones con transparencia: garantizar que cualquier excepción de cumplimiento esté documentada, justificada y aprobada para evitar responsabilidades legales.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Asume la responsabilidad global del cumplimiento legal y normativo de la organización.

4.1.2 Mantiene el Registro de Cumplimiento y garantiza que se conserve actualizado.

4.1.3 Revisa los contratos con clientes y garantiza que las obligaciones específicas se registren y se apliquen.

4.1.4 Aprueba excepciones a las obligaciones de cumplimiento únicamente cuando estén jurídicamente justificadas y existan controles compensatorios.

4.2 Asesores externos (por ejemplo, asesores jurídicos, de TI o consultores de cumplimiento)

4.2.1 Apoyan al Director General en la identificación de leyes, certificaciones y obligaciones aplicables (por ejemplo, RGPD, NIS2, ISO 27001).

4.2.2 Proporcionan orientación para interpretar nuevas normativas o cambios en la legislación vigente.

4.2.3 Pueden colaborar en actualizaciones de políticas, auditorías o respuesta ante violaciones de seguridad cuando exista exposición jurídica.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Revisión anual programada

9.1.1 Esta política debe ser revisada cada 12 meses por el Director General.

9.1.2 La revisión debe confirmar:

9.1.2.1 Su pertinencia respecto del contexto legal y contractual vigente.

9.1.2.2 La correcta incorporación de los acuerdos con clientes y de las obligaciones del servicio.

9.1.2.3 Su alineación con el Registro de Cumplimiento y otras políticas.

9.2 Actualizaciones motivadas por eventos

9.2.1 Se requiere una revisión inmediata si:

9.2.1.1 Una nueva ley o regulación pasa a ser aplicable (por ejemplo, una nueva norma de protección de datos).

9.2.1.2 Un cliente añade términos complejos de cumplimiento a su acuerdo.

9.2.1.3 Se produce una violación de seguridad o un incidente de incumplimiento.

9.2.1.4 La empresa se expande a un mercado o sector regulado.

9.3 Aprobación de actualizaciones y control de versiones

9.3.1 Todas las actualizaciones deben documentarse, someterse a control de versiones y ser aprobadas por el Director General.

9.3.2 Las versiones históricas deben conservarse con fines de auditoría y legales.

9.4 Comunicación de cambios

9.4.1 Se debe informar al personal y a los contratistas de los cambios en las políticas dentro de los 5 días hábiles siguientes a su aprobación.

9.4.2 Todo proveedor afectado debe también reconocer las condiciones actualizadas antes de continuar la prestación del servicio.

10. Políticas relacionadas y vinculaciones

10.1 Esta política se apoya y se aplica a través de las siguientes políticas SME:

10.1.1 P3S – Política de Uso Aceptable: previene conductas que puedan infringir términos legales o contractuales (por ejemplo, intercambio no autorizado de archivos).

10.1.2 P8S – Política de Concienciación y Formación en Seguridad de la Información: forma al personal sobre las obligaciones de cumplimiento y cómo evitar incumplimientos.

10.1.3 P14S – Política de conservación y eliminación de datos: garantiza prácticas de tratamiento de datos lícitas a lo largo del ciclo de vida de los datos.

10.1.4 P17S – Política de Protección de Datos y Privacidad: cumple los requisitos del RGPD y del tratamiento de datos de clientes.

10.1.5 P30S – Política de Respuesta a Incidentes: establece cómo responder a violaciones de seguridad de los datos o fallos de cumplimiento, incluidos los plazos de notificación.

10.1.6 P36S – Política de redes sociales y comunicaciones externas: garantiza que las comunicaciones públicas no infrinjan obligaciones legales o reglamentarias.

10.2 Cada política vinculada aplica una parte del marco de cumplimiento legal y debe aplicarse de manera conjunta.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – Acciones para abordar riesgos y oportunidades: incluye riesgos de cumplimiento.

11.1.2 Cláusula 8.1 – Planificación y control operacional: exige la ejecución de procesos que cumplan los requisitos legales y contractuales.

11.2 ISO/IEC 27002

11.2.1 Control 5.36 – Orienta a la organización en el mantenimiento de registros de obligaciones y en garantizar respuestas adecuadas a las necesidades legales y reglamentarias.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Política y procedimientos: exige políticas formales de cumplimiento.

11.3.2 PM-1 – Plan del programa de seguridad de la información: requiere la integración del cumplimiento legal en la planificación de seguridad.

11.3.3 CA-1 – Evaluación, autorización y supervisión.

11.3.4 AU-1 – Política de auditoría: exige el mantenimiento de evidencias de cumplimiento.

11.4 RGPD de la UE

11.4.1 Artículo 5 – Principios del tratamiento de datos, incluida la responsabilidad proactiva.

11.4.2 Artículo 6 – Base jurídica para el tratamiento.

11.4.3 Artículo 32 – Seguridad del tratamiento.

11.4.4 Artículo 33 – Notificación de violaciones de seguridad en un plazo de 72 horas.

11.5 Directiva NIS2 de la UE

11.5.1 Artículo 21(2)(a) y (f) – Políticas internas para la gestión del riesgo y el control reglamentario.

11.5.2 Artículo 23 – Aplicación y sanciones por incumplimientos.

11.6 DORA de la UE

11.6.1 Artículo 5(2) – Supervisión de la gestión del riesgo de las TIC.

11.6.2 Artículo 9(1) – Gobernanza interna del cumplimiento.

11.6.3 Artículo 17 – Acuerdos contractuales con proveedores de servicios de TIC.

11.7 COBIT 2019

11.7.1 APO12 – Riesgo gestionado: garantiza que los riesgos de cumplimiento se registren y se traten.

11.7.2 APO13 – Seguridad gestionada: cubre la aplicación basada en riesgos del cumplimiento reglamentario y contractual.

11.7.3 DSS01 – Operaciones gestionadas: exige preparación operativa para cumplir las obligaciones legales.