					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P37					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**

1. Propósito

1.1 Esta política establece el marco obligatorio para identificar, gestionar y cumplir todas las obligaciones legales, regulatorias y contractuales aplicables a la seguridad de la información, la privacidad de los datos y las funciones operativas de la organización.

1.2 El objetivo es prevenir incumplimientos que puedan dar lugar a sanciones económicas, responsabilidad legal, interrupción de las operaciones de la organización, daños reputacionales o medidas coercitivas por parte de las autoridades regulatorias.

1.3 Esta política respalda la integración de los requisitos de cumplimiento en la gobernanza, la gestión de riesgos, los flujos de trabajo operativos, los ciclos de vida de los proyectos y el diseño de sistemas.

1.4 Garantiza que todas las obligaciones aplicables, en las distintas jurisdicciones, sectores y ámbitos regulatorios, se documenten, evalúen, supervisen y apliquen claramente dentro de la organización.

2. Alcance

2.1 Esta política se aplica a todos los departamentos, funciones, unidades organizativas e individuos que actúen en nombre de la organización, incluidos:

2.1.1 Empleados fijos y temporales

2.1.2 Contratistas, consultores y becarios

2.1.3 Proveedores externos, encargados del tratamiento o socios que gestionen los datos, sistemas o responsabilidades regulatorias de la organización

2.1.4 Cualquier proceso de negocio, proyecto o iniciativa sujeto a control legal o regulatorio

2.2 Los ámbitos de cumplimiento regulados por esta política incluyen, entre otros:

2.2.1 Obligaciones de seguridad de la información y ciberseguridad (p. ej., ISO/IEC 27001, NIS2, DORA)

2.2.2 Legislación de protección de datos y privacidad (p. ej., RGPD de la UE, leyes sectoriales de privacidad)

2.2.3 Regulaciones sectoriales (p. ej., financiera, sanitaria, automoción, defensa)

2.2.4 Obligaciones contractuales derivadas de acuerdos de confidencialidad, acuerdos de nivel de servicio o acuerdos de tratamiento con terceros

2.2.5 Requisitos legales relacionados con la notificación de incidentes, la interacción con las fuerzas y cuerpos de seguridad y la transferencia internacional de datos

3. Objetivos

3.1 Garantizar que todas las leyes, reglamentos, normas y obligaciones contractuales aplicables se identifiquen, documenten, interpreten y apliquen en toda la organización.

3.2 Integrar los requisitos legales y regulatorios en el SGSI de la organización, los procesos de gestión de riesgos, los acuerdos con proveedores y el diseño de productos y servicios.

3.3 Proporcionar un mecanismo para supervisar de forma proactiva los cambios regulatorios y actualizar en consecuencia los controles y la documentación.

3.4 Definir responsabilidades claras para la supervisión del cumplimiento, el escalado de incumplimientos, la gestión de excepciones y la notificación externa.

3.5 Garantizar la trazabilidad y la solidez de la posición legal y regulatoria de la organización durante inspecciones, investigaciones o auditorías de certificación.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Asume la responsabilidad estratégica de la alineación legal y regulatoria en toda la organización.

4.1.2 Revisa y aprueba decisiones de cumplimiento de alto riesgo, incluidas las aceptaciones del riesgo y las controversias legales.

4.2 Responsable de Cumplimiento / Director Jurídico / Asesoría Jurídica

4.2.1 Mantiene el Registro de Obligaciones de Cumplimiento, en el que se relacionan todas las leyes, normas, certificaciones y cláusulas contractuales aplicables.

4.2.2 Realiza evaluaciones de impacto legal para nuevos servicios, mercados o flujos de datos.

4.2.3 Proporciona la interpretación autorizada de leyes y normas.

[... 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 de la política

9.1.1 Esta política debe revisarse al menos una vez por año natural para:

9.1.1.1 Garantizar la alineación continua con leyes actualizadas, normas del sector y marcos regulatorios

9.1.1.2 Validar la eficacia operativa con base en los hallazgos de auditoría y el historial de incidentes

9.1.1.3 Reflejar cambios en la organización (p. ej., nuevas jurisdicciones, sistemas o líneas de actividad)

9.2 Revisiones motivadas por eventos desencadenantes

9.2.1 Deben iniciarse revisiones intermedias cuando:

9.2.2 Se promulgue o actualice un nuevo requisito legal o regulatorio

9.2.3 Un incidente de cumplimiento o una auditoría revele deficiencias de la política

9.2.4 La organización entre en un nuevo mercado o línea de servicio regidos por marcos de cumplimiento específicos

9.2.5 Las tendencias regulatorias o las directrices de las autoridades indiquen cambios en la postura de riesgo

9.3 Titularidad y aprobación

9.3.1 El Departamento Jurídico y el Responsable de Cumplimiento comparten la responsabilidad de coordinar el proceso de revisión.

9.3.2 Las revisiones finales de esta política deben ser aprobadas por la Alta Dirección y registradas en el Registro de Cambios de Políticas, con las referencias asociadas de control de cambios y los planes de comunicación.

9.4 Control de versiones y comunicación

9.4.1 Toda versión actualizada de esta política debe:

9.4.1.1 Incluir un resumen de los cambios clave

9.4.1.2 Redistribuirse por los canales oficiales (p. ej., portal de políticas, LMS, boletines internos)

9.4.1.3 Requerir acuse de recibo de la política por parte del personal afectado, especialmente de quienes desempeñen funciones jurídicas, operativas, de seguridad y de gestión de proveedores

10. Políticas relacionadas y vinculaciones

10.1 Esta política opera conjuntamente con las siguientes políticas del SGSI de la organización y las refuerza:

10.1.1 P1 – Política de Seguridad de la Información: Establece los principios básicos de gobernanza que garantizan que todas las políticas de seguridad de la información, incluido el cumplimiento, estén alineadas con los requisitos estratégicos y regulatorios de la organización.

10.1.2 P2 – Política de funciones y responsabilidades de gobernanza: Define las autoridades de toma de decisiones, incluidas las funciones jurídicas y de cumplimiento responsables de la supervisión regulatoria y la rendición de cuentas.

10.1.3 P6 – Política de gestión de riesgos: Respalda la evaluación, la titularidad y la mitigación de los riesgos de cumplimiento legal y regulatorio en toda la organización.

10.1.4 P8 – Política de Concienciación y Formación en Seguridad de la Información: Garantiza que todo el personal esté informado de sus responsabilidades de cumplimiento y reciba formación específica por función.

10.1.5 P12 – Política de Gestión de Activos: Refuerza las obligaciones legales para gestionar y proteger activos regulados o sujetos a obligaciones contractuales, incluidos los que involucren datos personales e infraestructuras críticas.

10.1.6 P30 – Política de Respuesta a Incidentes: Regula las notificaciones legales obligatorias (p. ej., artículo 33 del RGPD de la UE) y los procedimientos de escalado en caso de incumplimiento o de un evento regulatorio.

10.1.7 P33 – Política de Supervisión de Auditoría y Cumplimiento: Proporciona actividades estructuradas de aseguramiento, incluidas pruebas de controles, remediación y recopilación de evidencias, necesarias para la verificación interna y externa del cumplimiento.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 4.2 – Comprensión de las necesidades y expectativas de las partes interesadas: exige la identificación e integración de requisitos legales y regulatorios en el SGSI.

11.1.2 Cláusula 5.1 – Liderazgo y compromiso: exige responsabilidad ejecutiva para establecer y mantener el cumplimiento legal en toda la organización.

11.1.3 Cláusula 5.3 – Funciones, responsabilidades y autoridades de la organización: garantiza la claridad de funciones para la supervisión jurídica y el cumplimiento regulatorio.

11.1.4 Anexo A, control 5.36 – Cumplimiento de requisitos legales y contractuales: establece la obligación de identificar y cumplir las obligaciones derivadas de leyes, reglamentos y contratos.

11.2 ISO/IEC 27002

11.2.1 Control 5.36: detalla directrices de implantación para mantener un registro de obligaciones de cumplimiento, validar requisitos regulatorios y garantizar una conservación estructurada de evidencias.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Política y procedimientos de planificación de la seguridad: exige que los mandatos de cumplimiento se integren en las estructuras de gobernanza y en la documentación.

11.3.2 PM-1 – Plan del programa de seguridad de la información: establece los controles regulatorios como componente del programa general de seguridad.

11.3.3 CA-7 – Monitorización continua: respalda la supervisión de la eficacia de los controles para cumplir requisitos legales y de política.

11.3.4 AU-9 – Protección de la información de auditoría: garantiza que los registros y logs de auditoría de cumplimiento estén protegidos y disponibles para inspección.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 5 – Principios relativos al tratamiento: exige licitud del tratamiento, transparencia y responsabilidad proactiva.

11.4.2 Artículo 6 – Licitud del tratamiento: exige bases jurídicas adecuadas para todas las actividades de tratamiento de datos.

11.4.3 Artículo 24 – Responsabilidad del responsable del tratamiento: establece responsabilidad directa para garantizar el cumplimiento regulatorio.

11.4.4 Artículo 32 – Seguridad del tratamiento: exige la implantación de medidas técnicas y organizativas (MTO) apropiadas.

11.4.5 Artículo 33 – Notificación de violaciones de seguridad de los datos personales: exige que las violaciones de seguridad de los datos personales se notifiquen a las autoridades competentes en un plazo de 72 horas.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículos 20–21: exigen que las entidades esenciales e importantes implanten gobernanza documentada, estrategias de cumplimiento legal y revisión continua de los riesgos legales.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 5(2) – Marco de gestión del riesgo de las TIC: exige la integración del cumplimiento legal dentro de funciones más amplias de gestión de riesgos y supervisión.

11.6.2 Artículo 19 – Riesgo de terceros de las TIC: impone requisitos legales específicos para gestionar obligaciones contractuales y regulatorias relacionadas con proveedores externos y plataformas.

11.7 COBIT 2019

11.7.1 APO12 – Gestionar el riesgo: incorpora el cumplimiento legal y regulatorio como componente crítico de la gobernanza del riesgo empresarial.

11.7.2 MEA03 – Supervisar el cumplimiento de requisitos externos: define la supervisión continua, la gestión de excepciones y la preparación para auditorías para todas las formas de obligaciones regulatorias.