					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P17					Título del documento: **Política de Protección de Datos y Privacidad**							
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

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1.3, 8.1, 10	Controles generales, técnicos y de mejora continua/protección de datos aplicables
ISO/IEC 27002:2022	Controles 5.34, 8.10, 8.11, 8.12	Controles para el tratamiento de PII, conservación, eliminación, anonimización y derechos de los interesados
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Requisitos de gobernanza, riesgo, gestión de accesos, registro de eventos, respuesta a brechas de seguridad y programa de privacidad
RGPD de la UE	Artículos 5, 6, 12–23, 25, 28, 30, 32–34; considerando 78	Todos los requisitos esenciales de privacidad, responsabilidad proactiva, derechos de los interesados, ejercicio de derechos, brechas de seguridad y principios de diseño y configuración por defecto
Directiva NIS2 de la UE	Artículo 21(2)(e), (f)	Controles de seguridad basados en riesgos para entidades esenciales e importantes
DORA de la UE	Artículos 6(2)(d), 11(1)(c), 15(1), 17	Gobernanza, riesgo de terceros y plazos para el tratamiento seguro
COBIT 2019	APO12, DSS01, DSS05, MEA	Gestión de riesgos, operaciones seguras y supervisión del cumplimiento

1. Propósito

1.1 Esta política establece principios organizativos obligatorios y requisitos técnicos para la protección de los datos personales y la aplicación de la privacidad desde el diseño en todos los entornos.

1.2 Formaliza las responsabilidades de la organización conforme a las normas internacionales y los marcos regulatorios, garantizando que los datos personales se recopilen, traten, conserven, compartan y eliminen de forma lícita, segura y transparente.

1.3 Esta política también refuerza el cumplimiento de las leyes y marcos de privacidad aplicables, incluidos el Reglamento General de Protección de Datos (RGPD) de la UE, la Directiva NIS2 de la UE, DORA de la UE, ISO/IEC 27001:2022 y COBIT 2019.

2. Alcance

2.1 Esta política se aplica a todas las unidades organizativas, al personal y a los sistemas implicados en el tratamiento de datos personales, incluidos:

2.1.1 Empleados, contratistas, consultores y proveedores de servicios externos.

2.1.2 Datos recopilados de fuentes internas y externas en todas las funciones de la organización.

2.1.3 Soportes físicos y digitales, incluidos servicios en la nube, plataformas SaaS, dispositivos móviles y registros en papel.

2.1.4 Todos los entornos, incluidos los sistemas de producción, desarrollo, pruebas y copia de seguridad en los que puedan existir datos personales.

2.2 Abarca todas las actividades de tratamiento reguladas por las leyes y normas de privacidad aplicables, incluidas, entre otras:

2.2.1 Recopilación, almacenamiento, uso, transmisión y eliminación de datos personales.

2.2.2 Gestión de los derechos de los interesados, documentación de la base jurídica y gestión del consentimiento.

2.2.3 Transferencias transfronterizas, notificación de brechas de seguridad e intercambio de datos con terceros.

2.2.4 Diseño seguro y aplicación de la privacidad por defecto en sistemas y procesos.

3. Objetivos

3.1 Garantizar el tratamiento lícito, transparente y sujeto a responsabilidad proactiva de los datos personales, en alineación con ISO/IEC 27001:2022 y los mandatos legales asociados.

3.2 Integrar los principios de privacidad desde el diseño y privacidad por defecto en todos los sistemas de información, servicios y procesos de la organización.

3.3 Aplicar medidas técnicas y organizativas (MTO) que salvaguarden la confidencialidad, integridad y disponibilidad de los datos personales durante todo su ciclo de vida.

3.4 Definir las funciones de gobernanza y las estructuras de responsabilidad proactiva para la protección de datos, incluidas las responsabilidades del Delegado de Protección de Datos (DPD), Seguridad de la Información, Asuntos Jurídicos y los propietarios de los datos.

3.5 Permitir el pleno cumplimiento de los artículos 5, 6, 25, 30 y 32 del RGPD, así como de los requisitos de reducción del riesgo y resiliencia en virtud de NIS2 y DORA.

3.6 Garantizar los derechos de los interesados, incluidos acceso, rectificación, supresión, limitación, portabilidad, oposición y protección frente a decisiones automatizadas.

3.7 Mitigar los riesgos regulatorios, reputacionales, legales y operativos derivados del acceso no autorizado, uso indebido o pérdida de datos personales.

4. Funciones y responsabilidades

4.1 Alta dirección

4.1.1 Proporciona supervisión estratégica y asigna recursos suficientes para respaldar el programa de privacidad.

4.1.2 Aprueba esta política y garantiza su aplicación en toda la organización.

4.2 Delegado de Protección de Datos (DPD)

4.2.1 Actúa con independencia para supervisar el cumplimiento de la normativa de protección de datos.

4.2.2 Mantiene el Registro de Actividades de Tratamiento (RAT) conforme al artículo 30 del RGPD.

4.2.3 Lidera la interlocución regulatoria, realiza Evaluaciones de Impacto relativas a la Protección de Datos (EIPD) y gestiona los procesos de notificación de brechas de seguridad.

4.2.4 Revisa las excepciones en materia de privacidad y mantiene el Registro de Excepciones de Privacidad.

[... 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 Esta política deberá revisarse al menos una vez al año o antes en las siguientes circunstancias:

9.1.1 Actualizaciones legales o regulatorias significativas (p. ej., modificaciones del RGPD o plazos de DORA)

9.1.2 Nuevos sistemas o actividades de tratamiento que involucren datos personales

9.1.3 Hallazgos de auditoría interna que indiquen deficiencias de la política

9.1.4 Incidentes materiales de brechas de seguridad u observaciones de la autoridad de control

9.2 Responsabilidades de revisión

9.2.1 El DPD deberá iniciar la revisión de la política, coordinándose con Asuntos Jurídicos, Riesgos, Seguridad de la Información y la alta dirección.

9.2.2 Todas las actualizaciones deberán registrarse en el Registro de Control Documental del SGSI y distribuirse a las partes interesadas afectadas.

9.3 Control de cambios

9.3.1 Toda revisión de esta política deberá ser aprobada formalmente por la alta dirección.

9.3.2 Las versiones obsoletas deberán archivarse de forma segura y la versión actualizada deberá incluir un historial de cambios documentado.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece los principios generales de gobernanza de seguridad que sustentan esta política de privacidad. P1 respalda la confidencialidad, integridad y disponibilidad de los datos personales en todos los sistemas y servicios.

10.2 P6 – Política de gestión de riesgos. Define la metodología de tratamiento de riesgos de la organización, esencial para evaluar riesgos de privacidad, procesos de EIPD y evaluaciones de riesgo residual exigidos por el RGPD y la cláusula 6.1.3 de ISO/IEC 27001.

10.3 P13 – Política de Clasificación y Etiquetado de Datos. Orienta la categorización de datos personales y sensibles, y constituye la base para aplicar controles de privacidad adecuados, incluida la aplicación de la conservación, la limitación del acceso y la eliminación segura.

10.4 P14 – Política de conservación y eliminación de datos. Respalda directamente los requisitos de privacidad de los artículos 5(1)(e) y 17 del RGPD, garantizando que los datos personales se conserven únicamente durante el tiempo necesario y se eliminen de forma segura conforme a las obligaciones legales.

10.5 P16 – Política de enmascaramiento de datos y seudonimización. Establece controles para reducir la capacidad de identificación de los datos personales mediante medidas técnicas como tokenización, enmascaramiento dinámico y seudonimización, aplicando así el artículo 32 del RGPD y el control 5.34 de ISO/IEC 27002.

10.6 P30 – Política de Respuesta a Incidentes. Define los protocolos obligatorios de respuesta a brechas de seguridad que se integran con la gestión y los plazos de notificación requeridos por los artículos 33 y 34 del RGPD.

10.7 P33 – Política de supervisión de auditoría y cumplimiento. Establece evaluaciones programadas de la eficacia del programa de privacidad, la aplicación de políticas y el seguimiento de acciones correctivas en todas las unidades organizativas y encargados del tratamiento externos.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.1 – Liderazgo y compromiso: establece la responsabilidad a nivel ejecutivo para proteger los datos personales y aplicar los principios de privacidad.

11.1.2 Cláusula 6.1.3 – Tratamiento de riesgos de seguridad de la información: respalda la identificación, evaluación y tratamiento de riesgos de privacidad mediante EIPD y excepciones.

11.1.3 Cláusula 8.1 – Planificación y control operacional: exige salvaguardas técnicas y procedimentales para garantizar que los datos personales se traten de forma segura.

11.1.4 Cláusula 10.1 – Mejora continua: exige la evaluación y adaptación periódicas del programa de privacidad.

11.2 Controles 5.34, 8.10, 8.11 y 8.12 de ISO/IEC 27002:2022: proporcionan directrices sobre el tratamiento de PII, la aplicación de la conservación, la eliminación, la anonimización y la transparencia respecto de los derechos de los interesados.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definen la gobernanza, las funciones, la responsabilidad proactiva y las responsabilidades de formación en privacidad.

11.3.2 PL-2, PL-8: exigen la integración de controles de privacidad en el ciclo de vida de los sistemas y en la arquitectura empresarial.

11.3.3 AC-2, AC-6: aplican el principio de mínimo privilegio y la gestión de cuentas para la protección de datos personales.

11.3.4 AU-2, AU-6, AU-9: exigen registro de eventos, trazabilidad e integridad de auditoría para el acceso a datos personales.

11.3.5 IR-4, IR-5, IR-6: definen procesos estructurados de detección, análisis y notificación para brechas de privacidad.

11.3.6 PM-1, PM-21, PM-23: establecen un programa integral de privacidad, alineado con los objetivos estratégicos de riesgo y gobernanza de datos.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículos 5, 6, 12–23, 25, 28, 30, 32–34: regulan el tratamiento lícito, la limitación de la finalidad, los derechos de los interesados, la responsabilidad proactiva, la protección de datos desde el diseño y por defecto, las obligaciones de terceros y la gestión de brechas de seguridad.

11.4.2 Considerando 78: refuerza los principios de privacidad desde el diseño.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(e) y (f): exige la implantación de controles de seguridad basados en riesgos y la protección de datos personales para entidades dentro del ámbito de entidades esenciales e importantes.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 6(2)(d): exige gobernanza interna para la gestión del riesgo de las TIC relacionada con el tratamiento de datos.

11.6.2 Artículo 11(1)(c): exige supervisión del riesgo de terceros para servicios relacionados con datos.

11.6.3 Artículos 15(1) y 17: exigen el tratamiento seguro de datos por parte de proveedores de servicios y comunicaciones oportunas a los supervisores tras incidentes relacionados con las TIC.

11.7 COBIT 2019

11.7.1 APO12 – Gestión de riesgos: integra el riesgo de privacidad en la supervisión más amplia del riesgo empresarial.

11.7.2 DSS01 – Operaciones gestionadas y DSS05 – Gestionar los servicios de seguridad: garantizan operaciones seguras, incluido el control de acceso, la conservación y la integridad del sistema.

11.7.3 MEA03 – Supervisión del cumplimiento: exige la revisión continua del estado de cumplimiento respecto de las obligaciones de privacidad regulatorias y basadas en políticas.