					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P17S					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Controles 5.34, 8.10–8.12	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
RGPD de la UE	Artículos 5, 6, 12-23, 30, 32-34	
Directiva NIS2 de la UE	Artículo 21(2)(e), 21(2)(f)	
DORA de la UE	Artículos 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Propósito

1.1. Esta política establece cómo la organización protege los datos personales de conformidad con las obligaciones legales, los marcos regulatorios y las normas internacionales de seguridad.

1.2. Garantiza que los datos personales, ya sean de clientes, personal o socios, se recopilen, utilicen, almacenen y eliminen de forma lícita, leal y segura.

1.3. Esta política también facilita el cumplimiento de ISO/IEC 27001:2022 y respalda la preparación de auditorías mediante la aplicación de un enfoque coherente y basado en riesgos para la protección de la privacidad.

1.4. Mediante esta política, la organización demuestra responsabilidad proactiva y refuerza la confianza de los clientes al priorizar la transparencia, la minimización de datos y una sólida gobernanza de la privacidad.

2. Alcance

2.1. Esta política se aplica a:

2.1.1. Todos los empleados, contratistas o proveedores de servicios que accedan a datos personales, los traten o los gestionen.

2.1.2. Cualquier sistema, aplicación o ubicación en la que se almacenen o transmitan datos personales.

2.1.3. Todos los datos personales, tanto si se almacenan electrónicamente, en papel, en sistemas en la nube o en dispositivos móviles.

2.2. Esta política se aplica a los datos relacionados con clientes, personal, proveedores y cualquier otra persona identificable.

2.3. Esta política permanece en vigor con independencia de que los datos se traten internamente o por proveedores de servicios externos.

3. Objetivos

3.1. Garantizar que los datos personales se traten de conformidad con las leyes de privacidad y las normas de seguridad, incluido el RGPD de la UE, la Directiva NIS2 de la UE e ISO/IEC 27001.

3.2. Proteger los datos personales frente a accesos no autorizados, uso indebido, alteración o pérdida mediante controles técnicos y organizativos claramente definidos.

3.3. Respetar los derechos de privacidad de las personas, incluido el derecho de acceso, rectificación y supresión de sus datos.

3.4. Establecer funciones y responsabilidades claras para la protección de datos dentro de la organización.

3.5. Aplicar la minimización de datos, la conservación segura y la eliminación oportuna en todos los sistemas y procesos.

3.6. Reducir el riesgo de incumplimiento, sanciones legales, daños reputacionales o pérdida de confianza de los clientes.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Aprueba esta política y garantiza su aplicación.

4.1.2. Proporciona los recursos necesarios para gestionar los riesgos de privacidad y responder a incidentes.

4.1.3. Asume la responsabilidad proactiva global del cumplimiento de las leyes y normas de privacidad.

4.2. Coordinador de Privacidad (interno o externalizado)

4.2.1. Mantiene los registros de las actividades de tratamiento de datos.

4.2.2. Responde a las solicitudes de ejercicio de derechos y a los requerimientos de los organismos reguladores.

4.2.3. Apoya las evaluaciones de riesgos, la formación y la implantación de la política.

4.2.4. Documenta los casos de brecha de seguridad y notifica a las autoridades cuando sea necesario.

[... 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. Revisiones programadas

9.1.1. Esta política debe revisarse al menos una vez cada 12 meses por el Coordinador de Privacidad y ser aprobada por el Director General.

9.1.2. La revisión debe evaluar la vigencia de la política, su alineación regulatoria y su eficacia operativa.

9.2. Desencadenantes de revisión extraordinaria

9.2.1. Las actualizaciones de la política también deben iniciarse en respuesta a:

9.2.1.1. Nuevas leyes de protección de datos o revisiones de estas, por ejemplo, el RGPD de la UE o DORA de la UE.

9.2.1.2. Incidentes de seguridad o brechas de privacidad que afecten a datos personales.

9.2.1.3. La puesta en marcha de nuevos sistemas, herramientas o servicios que traten datos personales.

9.2.1.4. Hallazgos materiales de auditoría o recomendaciones del regulador.

9.3. Control de cambios y comunicación

9.3.1. Todos los cambios en la política deben documentarse formalmente en un Registro de Cambios.

9.3.2. Las versiones revisadas deben distribuirse a todo el personal y a los contratistas que corresponda.

9.3.3. Las versiones archivadas deben conservarse para mantener la trazabilidad de auditoría del cumplimiento.

10. Políticas relacionadas y vinculaciones

10.1. Esta política opera conjuntamente con otras políticas de la pyme para crear un marco de privacidad completo y exigible:

10.1.1. P13S – Política de Clasificación y Etiquetado de Datos: garantiza que los datos personales se clasifiquen adecuadamente para que las medidas de protección de la privacidad puedan aplicarse en función del riesgo.

10.1.2. P14S – Política de Conservación y Eliminación de Datos: establece reglas claras sobre cuánto tiempo deben conservarse los datos personales y los métodos seguros para su eliminación una vez vencidos.

10.1.3. P16S – Política de Enmascaramiento de Datos y Seudonimización: especifica cómo deben transformarse los identificadores personales antes de utilizar los datos en un entorno no productivo o compartirlos externamente.

10.1.4. P30S – Política de Respuesta a Incidentes: cubre las medidas necesarias para responder a brechas de seguridad de los datos, incluida la notificación a reguladores y personas afectadas dentro de los plazos requeridos.

10.1.5. P2S – Política de Funciones y Responsabilidades de Gobernanza: aclara la estructura de responsabilidad proactiva y las funciones de toma de decisiones aplicables a la implantación y supervisión de la privacidad.

10.2. Estas políticas relacionadas deben revisarse y aplicarse conjuntamente para garantizar una cobertura integral de la privacidad en sistemas, personal y proveedores.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.1: exige que la Alta Dirección demuestre liderazgo y compromiso con la protección de los datos personales.

11.1.2. Cláusula 6.1.3: exige el tratamiento de los riesgos relacionados con el tratamiento de información personal.

11.1.3. Cláusula 8.1: exige la implantación de controles operativos para salvaguardar los datos durante todo su ciclo de vida.

11.2. ISO/IEC 27002

11.2.1. Control 5.34: proporciona directrices de implantación sobre la protección de la privacidad y el tratamiento seguro de la información de identificación personal.

11.2.2. Control 8.10: aborda la eliminación segura de datos personales para evitar su divulgación residual.

11.2.3. Control 8.11: respalda el uso de enmascaramiento y seudonimización para la minimización de datos.

11.2.4. Control 8.12: evita la fuga de datos no autorizada mediante controles sobre el acceso y el uso de los datos.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2: asigna funciones y responsabilidades para la gestión del riesgo de privacidad.

11.3.2. PL-5: exige la documentación de un plan de privacidad que cubra el uso y la protección de los datos.

11.3.3. AC-6: exige el principio de mínimo privilegio y controles de acceso para los datos personales.

11.3.4. IR-4: exige procesos de gestión de incidentes para brechas de seguridad que involucren datos personales.

11.4. RGPD de la UE

11.4.1. Artículo 5: define los principios fundamentales del tratamiento de datos lícito, leal y transparente.

11.4.2. Artículo 6: exige una base jurídica válida para cada actividad de tratamiento de datos personales.

11.4.3. Artículos 12–23: describen los derechos de los interesados, incluidos acceso, rectificación, supresión y oposición.

11.4.4. Artículo 30: exige registros de actividades de tratamiento.

11.4.5. Artículo 32: exige medidas de seguridad técnicas y organizativas adecuadas.

11.4.6. Artículos 33–34: establecen las obligaciones de notificación de brechas de seguridad a autoridades e interesados.

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(e): exige medidas para garantizar la protección de datos alineada con las políticas de ciberseguridad.

11.5.2. Artículo 21(2)(f): exige mecanismos para gestionar la seguridad de los datos personales y confidenciales en los sistemas TIC.

11.6. DORA de la UE

11.6.1. Artículo 6: exige marcos internos de gobernanza que gestionen el riesgo de los datos y su protección.

11.6.2. Artículo 15: obliga a las entidades financieras a garantizar que los proveedores externos protejan los datos personales y respalden el cumplimiento normativo.

11.6.3. Artículo 17: exige que las entidades garanticen que los sistemas TIC que tratan datos personales sean seguros, resilientes y estén supervisados.

11.7. COBIT 2019

11.7.1. APO12 – Gestionar el riesgo: exige la identificación y el tratamiento de los riesgos de privacidad y protección de datos.

11.7.2. DSS05 – Gestionar los servicios de seguridad: exige salvaguardas para evitar el acceso no autorizado a datos personales.

11.7.3. MEA03 – Supervisar el cumplimiento: exige que las organizaciones aseguren el cumplimiento continuo de las leyes de privacidad y protección de datos.