					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P29S					Título del documento: **Política de datos de prueba y entorno de pruebas - PYME**							
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 define cómo deben gestionarse los datos de prueba y los entornos de prueba para evitar exposiciones accidentales, violaciones de la seguridad de la información o interrupciones operativas durante las actividades de prueba.

1.2 Garantiza que los datos reales de clientes no se utilicen indebidamente durante las pruebas de software o sistemas y que los entornos de prueba estén segregados de los sistemas de producción tanto lógica como técnicamente.

1.3 Esta política está diseñada para ayudar a las pymes a cumplir los requisitos de certificación de ISO/IEC 27001 y la normativa aplicable en materia de protección de datos, manteniendo al mismo tiempo un enfoque práctico y exigible para organizaciones sin un equipo de TI dedicado.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los entornos de prueba (p. ej., servidores de preproducción, entornos sandbox y bancos de pruebas de desarrollo)

2.1.2 Todos los datos de prueba, ya sean creados manualmente, generados o derivados de sistemas de producción

2.1.3 Todo el personal que participe en actividades de prueba, incluidos empleados, contratistas, trabajadores autónomos y proveedores de servicios de TI

2.1.4 Cualquier prueba que pueda afectar a plataformas orientadas al cliente, sistemas internos de la organización o servicios de terceros

2.2 Cubre tanto los entornos técnicos como los procesos utilizados para dar soporte a:

2.2.1 El desarrollo de sitios web, aplicaciones y herramientas

2.2.2 Actualizaciones de sistemas, pruebas de configuración y pruebas de integración

2.2.3 Pruebas funcionales o de seguridad, automatizadas y manuales

3. Objetivos

3.1 Evitar el uso de datos reales e identificables de clientes en pruebas, salvo que estén anonimizados y cuenten con aprobación explícita.

3.2 Mantener una segregación estricta entre los sistemas de prueba y de producción para evitar exposiciones no intencionadas de datos o interferencias operativas.

3.3 Proteger los sistemas y datos de prueba frente a accesos no autorizados, divulgación accidental o reutilización entre entornos sin los controles adecuados.

3.4 Cumplir la normativa aplicable en materia de protección de datos (p. ej., RGPD de la UE, Directiva NIS2 de la UE), garantizando que todos los datos de prueba se traten de forma lícita, leal y segura.

3.5 Apoyar la preparación para auditorías externas y la certificación ISO/IEC 27001 de la organización mediante la documentación de las prácticas de prueba y la aplicación coherente de salvaguardas.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Tiene la responsabilidad general sobre la protección de los datos de prueba y la seguridad de los sistemas de prueba.

4.1.2 Aprueba cualquier uso de datos reales en pruebas tras confirmar la existencia de salvaguardas adecuadas (p. ej., anonimización o enmascaramiento de datos).

4.1.3 Verifica que las actividades de prueba estén debidamente documentadas y cumplan esta política.

4.2 Responsable del proyecto

4.2.1 Coordina el diseño y la ejecución de los procesos de prueba.

4.2.2 Garantiza que todos los miembros del equipo comprendan y cumplan esta política.

4.2.3 Confirma que los sistemas de prueba están configurados de forma segura antes del inicio de las pruebas.

4.2.4 Notifica al DG cualquier incidente relacionado con entornos de prueba o fuga de datos.

[... 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 al año por el Director General (DG). La revisión garantiza que la política se mantenga actualizada respecto de:

9.1.1.1 Cambios en herramientas, plataformas o entornos de desarrollo de software

9.1.1.2 Obligaciones legales actualizadas, incluidos los requisitos de protección de datos o resiliencia digital

9.1.1.3 Certificación de pymes y preparación para auditorías conforme a ISO/IEC 27001

9.2 Eventos desencadenantes para revisión extraordinaria

9.2.1 Deben realizarse revisiones adicionales tras:

9.2.1.1 Cualquier incidente que implique exposición de datos o compromiso en entornos de prueba

9.2.1.2 El uso de datos reales en pruebas, incluso si están anonimizados

9.2.1.3 La introducción de nuevos métodos de prueba, sistemas o proveedores

9.2.1.4 Actualizaciones regulatorias que afecten a la gestión de los datos durante las pruebas

9.3 Gestión del cambio y comunicación

9.3.1 El DG es responsable de:

9.3.1.1 Actualizar esta política y documentar cualquier revisión en el historial de versiones

9.3.1.2 Notificar las actualizaciones al personal, desarrolladores y proveedores de servicios pertinentes

9.3.1.3 Confirmar que todo el personal relacionado con las pruebas comprende y aplica las reglas más recientes

9.3.1.4 Mantener una versión accesible de la política vigente para fines de revisión y auditoría

9.4 Auditoría y documentación

9.4.1 Los registros de todas las revisiones de la política, las aprobaciones de uso de datos reales y cualquier justificación de excepción deben:

9.4.1.1 Conservarse de forma segura para fines de auditoría

9.4.1.2 Estar disponibles previa solicitud durante auditorías internas o de terceros

9.4.1.3 Revisarse anualmente para garantizar su coherencia con las prácticas de prueba

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe aplicarse de forma coordinada con las siguientes políticas para pymes a fin de mantener la seguridad y el cumplimiento durante las pruebas:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: define quién tiene la responsabilidad de supervisar el desarrollo, las pruebas y las responsabilidades de segregación de sistemas.

10.1.2 P4S – Política de control de acceso: regula la asignación, gestión y retirada de credenciales de acceso a sistemas de prueba.

10.1.3 P8S – Política de concienciación y formación en seguridad de la información: garantiza que el personal comprenda los riesgos de los datos de prueba, las prácticas de manejo seguro y la correcta segregación de entornos.

10.1.4 P13S – Política de clasificación y etiquetado de datos: facilita la clasificación clara de los datos de prueba y orienta las estrategias de anonimización o enmascaramiento.

10.1.5 P17S – Política de protección de datos y privacidad: se alinea con las obligaciones del RGPD de la UE, incluidas las salvaguardas relativas al tratamiento y almacenamiento de datos personales, también en entornos de prueba.

10.1.6 P24S – Política de desarrollo seguro: establece las expectativas generales de seguridad para los equipos de desarrollo, incluido el uso seguro de datos durante las fases de prueba.

10.1.7 P30S – Política de respuesta a incidentes: establece cómo responder a cualquier violación de seguridad o problema detectado en un entorno de prueba o causado por una gestión inadecuada de los datos de prueba.

10.2 Estas políticas forman un marco de seguridad unificado para apoyar la integridad de las pruebas, la minimización de datos y la plena alineación con ISO/IEC 27001 en las operaciones de desarrollo y aseguramiento de la calidad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1: exige evaluación de riesgos y acciones de tratamiento, incluidos los riesgos relacionados con las pruebas.

11.1.2 Cláusula 8.1: exige la planificación y el control de los procesos operativos, incluidos los entornos de configuración de sistemas de prueba.

11.2 ISO/IEC 27002

11.2.1 Control 8.28: exige que las organizaciones protejan los datos de prueba y garanticen que no contengan datos sensibles ni datos reales de producción.

11.2.2 Control 8.29: exige una segregación clara entre los entornos de desarrollo, prueba y producción.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11: cubre los requisitos de control para desarrollo y pruebas.

11.3.2 SA-12: aborda los riesgos de prueba en la cadena de suministro y las evaluaciones de seguridad.

11.3.3 SC-32: exige la separación de entornos y la protección de la confidencialidad e integridad de los datos de prueba.

11.4 Reglamento General de Protección de Datos (RGPD) de la UE

11.4.1 Artículo 5(1)(c): exige minimización de datos, incluido el uso exclusivo de los datos necesarios para las pruebas.

11.4.2 Artículo 25: exige privacidad desde el diseño, lo que incluye controles para entornos de prueba.

11.4.3 Artículo 32: exige el tratamiento seguro de los datos personales en todos los sistemas, incluidos los entornos no productivos.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(e, h): exige desarrollo seguro y pruebas de sistemas, especialmente cuando los servicios digitales están expuestos al riesgo cibernético.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9: destaca la importancia de la resiliencia operativa digital, incluida la realización segura de pruebas de sistemas TIC por pymes del sector financiero.

11.7 COBIT 2019

11.7.1 BAI07 – Gestionar la aceptación del cambio y la transición: incluye controles de prueba para validar nuevos sistemas y el tratamiento de datos.

11.7.2 DSS05 – Gestionar los servicios de seguridad: exige prácticas de prueba y desarrollo que eviten el uso indebido o la exposición de datos de la organización.