					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P29					Título del documento: **Política de datos de prueba y entornos de prueba**							
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 los requisitos obligatorios para la gestión de los entornos y los datos de prueba, a fin de garantizar la seguridad, la confidencialidad y la integridad operativa durante todo el ciclo de vida del desarrollo y las pruebas de software.

1.2. Su objetivo es prevenir el acceso no autorizado, la fuga de datos y la contaminación de los sistemas de producción derivados de una gestión inadecuada de los entornos de prueba o del uso de datos reales en las pruebas.

1.3. La política exige la gestión segura de los datos utilizados en pruebas, el endurecimiento de la infraestructura de prueba y el control de acceso basado en roles, en consonancia con las obligaciones regulatorias y contractuales aplicables.

2. Alcance

2.1. Esta política se aplica a todos los entornos de prueba, datos, herramientas y procesos utilizados para probar software, sistemas, aplicaciones e infraestructura en toda la organización.

2.2. Incluye:

2.2.1. Entornos de prueba aprovisionados on-premise, en la nube o mediante plataformas de terceros

2.2.2. Datos de prueba utilizados en pruebas funcionales, de rendimiento, de regresión y de seguridad

2.2.3. Pruebas manuales, mediante scripts o automatizadas (p. ej., pipelines de CI/CD)

2.2.4. Todo el personal implicado en las pruebas, incluidos equipos internos, proveedores y contratistas

2.3. La política aplica con independencia de la criticidad del sistema, del tipo de aplicación o de si el desarrollo se realiza internamente o está externalizado.

3. Objetivos

3.1. Prevenir el uso de datos de producción, sensibles o regulados en entornos de prueba (p. ej., información de identificación personal (PII), datos del titular de la tarjeta), salvo que estén anonimizados o cuenten con una aprobación específica.

3.2. Garantizar la segregación completa de red y accesos entre los entornos de prueba y de producción para evitar accesos no autorizados a los datos o la contaminación de sistemas.

3.3. Exigir cifrado, enmascaramiento de datos o generación de datos sintéticos cuando se requieran datos representativos con fines de prueba.

3.4. Reducir la probabilidad de incumplimientos, exposición de datos de clientes o interrupciones operativas derivadas de datos o entornos de prueba inseguros.

3.5. Alinear la gestión de datos de prueba con normas del sector (ISO, NIST, COBIT) y con reglamentos como el RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

4. Funciones y responsabilidades

4.1. Director de Seguridad de la Información (CISO)

4.1.1. Es el propietario de esta política y debe aplicar salvaguardas técnicas y administrativas para los datos y entornos de prueba.

4.1.2. Aprueba el uso de datos reales o sensibles en pruebas con la debida justificación y controles compensatorios.

4.2. Responsables de QA/Pruebas

4.2.1. Coordinan la planificación de las pruebas y garantizan que todas las actividades de prueba cumplan los requisitos de esta política.

4.2.2. Verifican la segregación adecuada, los accesos y la preparación de datos para cada fase de pruebas.

[... 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 debe revisarse anualmente y actualizarse cuando sea necesario para reflejar:

9.1.1. Cambios en los requisitos regulatorios (p. ej., RGPD de la UE, DORA de la UE, Directiva NIS2 de la UE)

9.1.2. La adopción de nuevas herramientas, plataformas o pipelines de automatización para pruebas

9.1.3. Hallazgos de auditoría interna o recomendaciones posteriores a incidentes

9.1.4. La ampliación de procesos de desarrollo o QA que modifiquen la gestión de datos de prueba o el uso de entornos

9.2. El Director de Seguridad de la Información es responsable de iniciar proactivamente la revisión en colaboración con:

9.2.1. Responsables de QA/Pruebas

9.2.2. Responsables de DevOps e Infraestructura

9.2.3. Equipos de Desarrollo de Aplicaciones

9.2.4. Delegado de Protección de Datos (DPO) y área jurídica

9.3. Todas las revisiones deben:

9.3.1. Estar sujetas a control de versiones y almacenarse en el repositorio documental central

9.3.2. Comunicarse al personal afectado a través de canales formales (p. ej., notificaciones del SGSI, sesiones informativas de equipo)

9.3.3. Vincularse a actualizaciones de normas técnicas, controles y procedimientos operativos asociados

9.4. Deben realizarse revisiones intermedias basadas en desencadenantes inmediatamente después de cualquier:

9.4.1. Fuga de datos o brecha de seguridad que afecte a entornos de prueba

9.4.2. No conformidad de auditoría relacionada con la gestión de datos de prueba

9.4.3. Cambio significativo en las obligaciones legales o en la arquitectura de TI

10. Políticas relacionadas y vinculaciones

10.1. Esta política está estrechamente integrada con las siguientes políticas para garantizar la gestión segura y conforme de los datos y entornos de prueba:

10.1.1. P1 – Política de Seguridad de la Información: establece los principios generales de seguridad que rigen la protección de los datos de prueba y la gestión de entornos.

10.1.2. P5 – Política de Gestión de Cambios: se aplica a la creación, actualización y retirada de entornos de prueba y pipelines de despliegue.

10.1.3. P13 – Política de Clasificación y Etiquetado de Datos: guía la selección de datos de prueba y la aplicación de controles según la sensibilidad.

10.1.4. P14 – Política de Conservación y Eliminación de Datos: define los plazos de conservación y los requisitos de eliminación segura para los conjuntos de datos de prueba.

10.1.5. P15 – Política de Copias de Seguridad y Restauración: establece prácticas obligatorias de copia de seguridad y validación de copias de seguridad para los entornos de prueba.

10.1.6. P18 – Política de Controles Criptográficos: especifica los estándares de cifrado obligatorios para los datos en reposo y en tránsito dentro de las plataformas de prueba.

10.1.7. P22 – Política de Registro y Supervisión: regula la visibilidad y la detección de anomalías en las actividades de los entornos de prueba.

10.1.8. P30 – Política de Respuesta a Incidentes: define el escalado y la remediación para brechas de seguridad o incidentes que afecten a sistemas de prueba.

10.1.9. P33 – Política de Supervisión de Auditoría y Cumplimiento: permite validar el cumplimiento de la política y el aseguramiento continuo.

11. Normas y marcos de referencia

11.1. Esta política se alinea con normas globales de ciberseguridad y marcos regulatorios que exigen la gestión segura de los datos de prueba y la protección de los entornos no productivos.

11.2. ISO/IEC 27001:

11.2.1. Cláusula 8.1: exige la planificación y el control seguros de los datos y entornos de prueba.

11.3. ISO/IEC 27002:2022 – Controles 8.28–8.29:

11.3.1. Anexo A, control 8.28 – Datos de prueba seguros: exige la protección de los datos de prueba utilizados en las fases de desarrollo y pruebas mediante anonimización, enmascaramiento o generación sintética.

11.3.2. Anexo A, control 8.29 – Protección de los entornos de prueba: exige la segregación respecto de producción, controles de acceso y endurecimiento del entorno para los sistemas de prueba.

11.3.3. Estos controles establecen requisitos para gestionar de forma segura los datos utilizados durante las pruebas y para proteger los sistemas no productivos frente al uso indebido, el compromiso o la contaminación.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – Pruebas y evaluación del desarrollador: establece expectativas para procedimientos de prueba seguros y repetibles con controles de datos adecuados.

11.4.2. SC-28 – Protección de la información en reposo: se alinea con el cifrado de los datos de prueba almacenados en sistemas no productivos.

11.4.3. SC-32 – Integridad de la información: respalda la validación de datos, la prevención de la corrupción y los controles de entrada/salida durante las pruebas.

11.5. RGPD de la UE (2016/679):

11.5.1. Artículo 5 – Minimización de datos: prohíbe el uso innecesario de datos personales en pruebas.

11.5.2. Artículo 25 – Privacidad desde el diseño: exige aplicar técnicas de protección de datos desde el inicio del ciclo de desarrollo y pruebas.

11.5.3. Artículo 32 – Seguridad del tratamiento: exige salvaguardas para entornos de prueba que traten datos personales o sensibles.

11.6. Directiva NIS2 de la UE (2022/2555):

11.6.1. Artículo 21(2)(e, h): exige procesos seguros de desarrollo y pruebas de software, con énfasis en la protección frente al acceso no autorizado y la fuga de datos.

11.7. DORA de la UE (2022/2554):

11.7.1. Artículo 9 – Sistemas y protocolos de TIC: exige que los procesos de prueba respalden la resiliencia y protejan los datos operativos frente al compromiso o la divulgación no autorizada.

11.8. COBIT 2019:

11.8.1. DSS05 – Gestionar los servicios de seguridad: respalda la aplicación de políticas de seguridad en todos los entornos, incluidos los no productivos.

11.8.2. BAI07 – Gestionar la aceptación y transición del cambio: cubre el proceso formal de transición de pruebas a producción, incluidos los controles sobre datos y entornos.