

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE PROTECCIÓN DE DATOS DE PRUEBA	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 1 de 2

1 Propósito

Establecer las reglas básicas para el uso y manejo de datos utilizados en ambientes de desarrollo, prueba o control de calidad, evitando la exposición no autorizada de información personal o sensible.

2 Alcance

Esta política aplica a cualquier ambiente distinto del entorno productivo (desarrollo, staging, pruebas automatizadas, pruebas manuales, integración continua, etc.), en el cual se utilicen datos representativos de la operación real.

3 Reglas de aplicación

- No se permite el uso de **datos reales** de usuarios, clientes, proveedores o empleados en ambientes de prueba, a menos que exista **autorización expresa** y justificada por el Responsable de Seguridad de la Información.
- En caso de requerirse información real con fines técnicos:
 - Se deberán eliminar o modificar campos como nombres completos, RUT, correos reales, direcciones y contraseñas.
- Las pruebas deben realizarse con:
 - Generadores de datos ficticios o aleatorios.
 - Registros de prueba ya preparados por el equipo técnico.
 - Claves o tokens controlados, no operativos.
 -
- Los entornos de prueba deben estar:
 - Aislados de los entornos productivos.
 - Restringidos a usuarios autorizados.
 - Sin acceso externo público o sin autenticación.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	POLÍTICA DE PROTECCIÓN DE DATOS DE PRUEBA	
VIGENCIA: 25/06/2024	VERSIÓN: 1	PÁG. 2 de 2

- Los registros generados durante las pruebas que contengan datos sensibles deben ser eliminados al finalizar la fase de prueba.

4 Supervisión y cumplimiento

La revisión del cumplimiento de esta política será responsabilidad del equipo de desarrollo y del área de seguridad. Cualquier incumplimiento debe ser notificado y documentado como un incidente.



CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024