1. Introducción

Esta política define los principios básicos que deben seguirse para el diseño y la construcción de sistemas seguros, minimizando riesgos desde la fase de desarrollo hasta su operación. La política aplica a todo sistema nuevo o actualizado desarrollado internamente o por terceros.

2. Diseño seguro

El diseño de sistemas en Safe Comercial debe considerar desde el inicio la protección de los datos personales y las funciones críticas para esto se aplicarán los siguientes lineamientos:

- El sistema debe tener una **arquitectura modular** y separada:
    - Backend (FastAPI) aislado del frontend (React con Astro).
    - Microservicio local de desencriptación separado del flujo general.
    - Control de acceso basado en roles.

- Toda la **información sensible (contraseñas, identificaciones)** debe gestionarse de forma controlada, sin exposición en el cliente o en transmisiones sin protección.

- El intercambio de datos entre el microservicio local, APIs debe estar protegido con **TLS, autenticación por token o control de IP**.

3 Desarrollo seguro

- El código debe cumplir con las reglas definidas de desarrollo seguro.
- Toda lógica que maneje autenticación, sesión, cifrado o integridad de datos debe ser cuidadosamente implementada y revisada.
- El equipo debe utilizar versiones seguras y actualizadas de librerías, frameworks y dependencias.

4 Entorno de desarrollo seguro *(A.14.2.6)*

- Los entornos de desarrollo, pruebas y producción deben estar claramente separados.
- Solo personal autorizado puede tener acceso a los entornos de desarrollo.
- Los sistemas de desarrollo deben estar protegidos contra malware y accesos externos no controlados.
- El código de desarrollo no debe contener datos reales de usuarios ni claves de producción.

5 Validación previa a la entrega

- Antes de su paso a producción, todo sistema debe:
- Ser revisado técnicamente por un par.
- Pasar pruebas funcionales completas.
- Cumplir con los requisitos de seguridad mínimos definidos.

6 Responsabilidades

- Los desarrolladores deben aplicar estas prácticas en cada etapa del ciclo de vida del software.
- El área de TI debe garantizar el aislamiento y protección del entorno de desarrollo.
- Seguridad de la Información puede auditar el cumplimiento y proponer mejoras.

CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024