1. OBJETIVO

Garantizar que el desarrollo de software en Doc Flow se realice siguiendo prácticas de seguridad basadas en OWASP, para proteger la información y mitigar riesgos de manera rápida y efectiva.

2. ALCANCE

Esta política se aplica a todas las aplicaciones desarrolladas, mantenidas o adquiridas por Doc Flow, así como a todo el personal involucrado en su desarrollo, pruebas, implementación y mantenimiento.

3. RESPONSABILIDADES

Para garantizar la correcta implementación y cumplimiento de esta política, se definen las siguientes responsabilidades:

3.1. Oficial de Seguridad de la Información

- Definir y actualizar lineamientos de seguridad basados en OWASP.
- Supervisar el cumplimiento mediante revisiones simples y auditorías puntuales.
- Brindar asesoría en seguridad al equipo de desarrollo.

3.2. Equipo de Desarrollo de Software

- Seguir prácticas seguras de desarrollo según el OWASP Top 10.
- Realizar revisiones de código (manual y con herramientas SAST) antes de la implementación.
- Utilizar únicamente librerías y frameworks aprobados.
- Reportar vulnerabilidades detectadas durante el desarrollo.

3.3. Jefe de TI

- Garantizar la segregación de ambientes (Desarrollo, Pruebas y Producción).
- Implementar controles simples de acceso para producción.
- Monitorear incidentes de seguridad y apoyar en la remediación de vulnerabilidades críticas.

3.4. Todos los Colaboradores Involucrados en el Desarrollo de Software

- Cumplir con lo establecido en esta política.
- Reportar cualquier anomalía o posible brecha de seguridad.
- Participar en las capacitaciones sobre seguridad.

4. DEFINICIÓN

El Ciclo de Vida del Desarrollo de Software (SDLC, por sus siglas en inglés) es un proceso estructurado que guía el desarrollo de software desde la planificación hasta el mantenimiento. Su objetivo es asegurar que el software sea eficiente, seguro y cumpla con los requisitos de calidad.

5. ABREBIATURAS

TI: Tecnología de la información.
OWAST: Open Web Application Security Project.

6. FRECUENCIA DE EJECUCION

Esta política se aplicará en cada nuevo desarrollo y actualización de software de Doc Flow.

7. LINEAMIENTOS

7.1. Documentación y Framework de Aplicaciones

- Adoptar un enfoque SDLC simplificado basado en OWASP, integrando controles de seguridad desde la planificación hasta el despliegue.

7.2. Requerimientos de Seguridad y Mejores Prácticas

Las aplicaciones deberán seguir los lineamientos como:

- ✓ OWASP Top 10: Aplicar las prácticas para mitigar las vulnerabilidades más comunes.
- ✓ Validación de Entradas y Salidas: Implementar filtros y sanitización para prevenir inyecciones.
- ✓ Autenticación y Sesiones: Usar métodos de autenticación simples y gestionar sesiones de forma segura (cookies con HttpOnly y Secure).
- ✓ Cifrado: Proteger datos sensibles en tránsito (HTTPS) y, en lo posible, en reposo con técnicas de cifrado.
- ✓ Gestión de Errores: Registrar y manejar errores de forma que no se exponga información sensible.

7.3 Establecimiento De Métricas (Kpis/Kris)

Para evaluar la seguridad del desarrollo, se definirán métricas como:

- Número de vulnerabilidades detectadas en revisiones de código.
- Tiempo de remediación de vulnerabilidades críticas.
- Cumplimiento en revisiones de seguridad en cada entrega.

7.4 - Gestión De Accesos En Producción

- Mantener separados los ambientes de Desarrollo, Pruebas y Producción.
- Restringir el acceso a producción personal autorizado mediante controles.

7.5 Gestión de Servicios y Librerías

Se utilizarán únicamente librerías aprobadas y con mantenimiento activo.
Se realizará análisis de dependencias según lo recomendado por OWASP para detectar vulnerabilidades.
Se evitarán librerías obsoletas o con vulnerabilidades conocidas.

7.6 Revisiones de Código

- Realizar revisiones manuales y emplear herramientas SAST (integradas en el CI/CD) antes de implementar cambios.
- Ejecutar pruebas de seguridad simples (DAST o escaneos de vulnerabilidades) en entornos de pruebas.

7.7 Capacitación para Desarrolladores

- Se realizarán capacitaciones periódicas sobre seguridad en el desarrollo**.**
- Se promoverá el uso de herramientas de análisis de seguridad y prácticas seguras de programación.
- Se incluirán entrenamientos específicos sobre **OWASP, DevSecOps y normativas aplicables**.

7.9 Controles en Ambientes No Productivos

- Se implementarán controles para evitar exposición de datos sensibles en entornos de desarrollo y prueba.
- Se usarán datos ficticios o anonimizados para pruebas.

- Los accesos a estos entornos serán monitoreados y restringidos según perfil de usuario.

7.10. Controles en el Uso de Información de Producción

- Está prohibido utilizar información real de producción en entornos de desarrollo o prueba.
- Si se requiere información para pruebas, se aplicarán técnicas de anonimización o enmascaramiento de datos.

8.- INCUMPLIMIENTOS

DOC FLOW S.A.C. hará responsable al colaborador de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento. La empresa se reserva el derecho de evaluar periódicamente el cumplimiento de esta política. Cualquier acción disciplinaria derivada del incumplimiento de esta será considerada de acuerdo con los procedimientos establecidos.

El colaborador que no cumpla con el uso correcto de los activos será directamente responsable de las sanciones legales derivadas de sus propios actos y de los costos y gastos en que pudiera incurrir la empresa en defensa por el uso no autorizado o indebido de los recursos.

9. REGISTRO DE CAMBIOS

Revisión	Fecha	Modificación
01	29-03-2025	Edición Inicial

ELABORACIÓN	REVISIÓN	APROBACIÓN
.....	.....	.....
Jhoel Gutierrez	Leonardo Chamochumbi	Anibal Robles
	Gerente de Operaciones	**Gerente General**
		Fecha: 29/03/2025

Jefe de Tecnologías de Información Fecha: 29/03/2025	Fecha: 29/03/2025	

.