

 RST Asociados	POLÍTICAS Y PROCEDIMIENTOS DE DESARROLLO SEGURO	Clasificación: 1
		Versión: 1.0
		Fecha de Actualización: 31- Ener-2025

OBJETIVO Establecer directrices para garantizar la seguridad de la información en el ciclo de vida del desarrollo de software, alineadas con el Sistema de Gestión de Seguridad de la Información por medio de la norma ISO 27001 y del Sistema de Gestión de la Calidad por medio de la norma ISO 9001 vigente.

ALCANCE Esta política aplica a todos los sistemas, aplicaciones y software desarrollados interna o externamente, incluyendo terceros y proveedores.

PRINCIPIOS DE DESARROLLO SEGURO

- **Security by Design:** Incorporar controles de seguridad desde las primeras etapas del desarrollo.
- **Menos privilegios:** Aplicar el principio de acceso mínimo necesario.
- **Defensa en profundidad:** Implementar múltiples capas de seguridad.
- **Ciclo de vida seguro (SDLC):** Adoptar metodologías seguras, para los desarrollos internos se utilizará SecDevOps.
- **Cumplimiento normativo:** Seguir regulaciones como ISO 27001, GDPR, y otras aplicables, acorde con las necesidades del desarrollo a generar.

POLÍTICAS GENERALES

1.1. **Control de acceso al código fuente**

- Restringir el acceso al código fuente basado en roles y necesidades.
- Mantener registros de acceso y modificaciones.

1.2. **Revisión y análisis de código**

- Implementar revisiones de código seguros (SAST, DAST).
- Automatizar análisis de vulnerabilidades en el código.

1.3. **Gestión de dependencias**

- Usar repositorios seguros y evitar dependencias obsoletas.
- Asegurar la implementación de espacios para el desarrollo en ambientes independientes, ya sea de desarrollo, pruebas, y operación.
- Evaluar vulnerabilidades en librerías y frameworks.

1.4. **Pruebas de seguridad**

- Realizar pruebas de seguridad en cada fase del desarrollo.
- Implementar pruebas de penetración antes de la implementación.

1.5. **Protección de datos en desarrollo y pruebas**

Elaborado por: Líder de data y Analytics	Revisado por: Director del SGC	Aprobado por: Líder de data y Analytics
Fecha: 23/01/2025	Fecha: 30/01/2025	Fecha: 31/01/2025

 RST Asociados	POLÍTICAS Y PROCEDIMIENTOS DE DESARROLLO SEGURO	Clasificación: 1
		Versión: 1.0
		Fecha de Actualización: 31- Ene-2025

- Se prohíbe el uso de datos reales en entornos de prueba salvo requerimiento explícito del cliente interno o externo, acorde con la naturaleza del desarrollo a generar.
- Aplicar siempre el enmascaramiento o anonimizado de datos.

1.6. **Gestión de cambios y despliegue seguro**

- Evaluar el impacto en seguridad de la información y del cumplimiento a los requisitos funcionales y de desempeño esperados antes de cada cambio.
- Implementar revisiones antes de cada despliegue.

2. **PROCEDIMIENTOS**

2.1. **Fase de Planificación**

- Identificar requisitos de seguridad desde el inicio.
- Evaluar riesgos de seguridad del proyecto.
- Definir el plan de trabajo y tipo de pruebas a efectuar, acorde con las necesidades del proyecto a desarrollar.

2.2. **Fase de Diseño**

- Aplicar principios de codificación segura.
- Definir controles de autenticación y autorización.

2.3. **Fase de Desarrollo**

- Implementar revisiones de código y pruebas automatizadas.
- Aplicar controles de acceso a entornos de desarrollo.

2.4. **Fase de Pruebas**

- Ejecutar pruebas de seguridad automatizadas y manuales.
- Validar cumplimiento de los criterios de seguridad.
- Verificar el cumplimiento a los requisitos funcionales y de desempeño para el proyecto o desarrollo a efectuar.

2.5. **Fase de Implementación y Mantenimiento**

- Monitorear y responder a incidentes de seguridad.
- Actualizar regularmente las dependencias y parches de seguridad.

3. **ROLES Y RESPONSABILIDADES**

- **Equipo de Desarrollo:** Aplicar las prácticas de seguridad definidas.
- **Equipo de Seguridad:** Revisar y validar la seguridad del software.

 RST Asociados	POLÍTICAS Y PROCEDIMIENTOS DE DESARROLLO SEGURO	Clasificación: 1
		Versión: 1.0
		Fecha de Actualización: 31- Ene-2025

- **Auditoría Interna:** Evaluar el cumplimiento de la política.
- **Proveedores Externos:** Cumplir con los requisitos de desarrollo seguro.

4. CUMPLIMIENTO Y SANCIONES

El incumplimiento de estas políticas podrá derivar en sanciones disciplinarias y correctivas según lo establecido por la organización en su reglamento interno de trabajo.

5. REVISIÓN Y MEJORA CONTINUA

Esta política será revisada anualmente y actualizada según la evolución de amenazas y tecnologías.

CONTROL DE CAMBIOS.		
VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1.0	Emisión inicial.	31-Enero-2025