1. Objetivo

El desarrollo de software seguro es una prioridad crítica para nuestra organización, ya que garantiza la protección de los datos confidenciales de la empresa, la integridad de los sistemas y la confianza de nuestros clientes.

Esta política establece los estándares y procedimientos que deben seguir todos los equipos de desarrollo de software para garantizar la seguridad de los productos y aplicaciones.

- **Garantizar** que todos los productos de software desarrollados por la empresa cumplan con los más altos estándares de seguridad.
- **Minimizar** el riesgo de vulnerabilidades y exposición a amenazas cibernéticas en el software.
- **Proteger** la confidencialidad, integridad y disponibilidad de los datos de la empresa y de nuestros clientes.
- **Fomentar** una cultura de desarrollo seguro dentro de los equipos de desarrollo de software.

2. Involucrados

TI/ Dep. Desarrollo / Dir. Op

3. Alcance

Esta política se aplica a todos los empleados que participan en el desarrollo de software para la organización, independientemente de la ubicación o la naturaleza del proyecto.

4. Procedimientos

4.1. Formación

Todos los miembros del equipo de desarrollo deben recibir formación en seguridad de la información y prácticas de desarrollo seguro de forma regular.

Se deben proporcionar recursos y material educativo sobre seguridad de TI para mantener actualizado al personal sobre las últimas amenazas y mejores prácticas.

4.2. Análisis de Riesgos y Diseño Seguro

Antes de iniciar cualquier proyecto de desarrollo de software, se debe realizar un análisis de riesgos para identificar y evaluar posibles amenazas y vulnerabilidades.

El diseño del software debe incluir consideraciones de seguridad desde el principio, asegurando la incorporación de controles de seguridad adecuados en la arquitectura y el diseño.

4.3. Desarrollo y Codificación Segura

Los desarrolladores deben seguir las mejores prácticas de codificación seguro, como la validación de entrada, la sanitización de datos y la prevención de vulnerabilidades conocidas.

4.4. Pruebas de Seguridad

Todos los proyectos de software deben someterse a pruebas exhaustivas de seguridad, incluyendo pruebas de penetración, análisis estático y dinámico del código, y pruebas de vulnerabilidades.

Se deben realizar pruebas de forma regular durante todo el ciclo de vida del desarrollo de software, desde la fase de desarrollo hasta la producción.

4.5. Revisión de Código y Gestión de Dependencias

Todas las modificaciones de código deben revisarse por pares para identificar y corregir posibles problemas de seguridad antes de la implementación.

Se debe realizar una gestión adecuada de las dependencias del software para garantizar que se utilicen versiones actualizadas y seguras de las bibliotecas y frameworks.

4.6. Protección de Datos y Privacidad

Se deben implementar medidas de protección de datos, como la encriptación de datos sensibles y el control de acceso adecuado, para proteger la confidencialidad e integridad de la información.

5. Responsabilidades

El equipo de gestión de TI es responsable de establecer y hacer cumplir esta política, así como de proporcionar recursos y apoyo para su implementación.

Los gerentes de proyecto son responsables de garantizar que se cumplan los estándares de desarrollo seguro en sus proyectos y de asignar los recursos necesarios para implementar medidas de seguridad adecuadas.

Los líderes de equipo de desarrollo son responsables de asegurar que sus equipos sigan las prácticas de desarrollo seguro y de proporcionar orientación y apoyo en materia de seguridad.

Los desarrolladores son responsables de adherirse a las directrices y procedimientos establecidos en esta política y de informar de cualquier problema de seguridad identificado durante el desarrollo del software.

6. Cumplimiento

Todos los equipos de desarrollo de software deben cumplir con los estándares y procedimientos establecidos en esta política.

Esta política será revisada periódicamente para asegurar su efectividad y relevancia con respecto a los cambios en la tecnología y las amenazas emergentes de seguridad de la información.

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del empleo, y puede exponer a la organización a riesgos de seguridad significativos.