Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Lineamiento	L-SGSI-012	Fecha:	14/08/2018	**Página #:**	1 de 3
Título:	Lineamiento de Desarrollo Seguro				

Lineamiento de Desarrollo Seguro

1.0 PROPÓSITO

El propósito de este documento es establecer los lineamientos para el desarrollo de software del Poder Judicial, con el fin de garantizar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información.

2.0 ALCANCE

Este lineamiento aplica para todas las personas que laboran en el Poder Judicial y terceros que desarrollan software institucional.

3.0 TÉRMINOS Y DEFINICIONES

Para mayor claridad sobre el contenido de este lineamiento, se debe tener en cuenta los siguientes términos y definiciones:

- Ciclo de vida de desarrollo: conjunto de fases que permiten que el software desarrollado cumpla con los requerimientos descritos y genere los resultados planteados.
- Separación de funciones: control administrativo utilizado para prevenir el hecho que una persona realice una actividad crítica de forma individual.
- Software: programas utilizados para operar las computadoras y dispositivos relacionados, incluyendo aplicaciones y sistemas.

4.0 RESPONSABILIDADES

Con el fin de cumplir con los requisitos de este lineamiento se describen las siguientes responsabilidades:

1) Área de Informática de Gestión y de Sistemas de la DTIC

a. Establecer una metodología única para el desarrollo de software, en donde se considere la seguridad de la información durante todo el ciclo de vida de los programas.

b. Realizar las labores de desarrollo de los programas del Poder Judicial, siguiendo la metodología y mejores prácticas de desarrollo seguro de software.

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

c. Implementar controles para evitar la fuga de información durante el proceso de desarrollos contratados.

2) Dirección de Tecnología de Información y Comunicaciones

a. Velar porque se implementen los controles de seguridad requeridos durante el desarrollo de software del Poder Judicial.

4.0 PAUTAS

a. Cualquier desarrollo o cambio en los programas nuevos o existentes, debe contemplar un estudio de requerimientos técnicos y de seguridad de la información en las primeras fases del ciclo de vida de desarrollo de software.

b. Cuando aplique, se deben tomar en cuenta los principios de ingeniería para sistema seguro durante cada una de las etapas del ciclo de vida de desarrollo de software.

c. Se debe considerar la separación de funciones críticas en la autorización del acceso a los ambientes de desarrollo, pruebas y producción.

d. Todo software desarrollado por la institución o terceros, debe someterse a pruebas de seguridad automatizadas y manuales, antes de realizar el pase del programa al ambiente de producción.

e. Todo software desarrollado por la institución o terceros, debe generar registros de auditoría y contar con los controles para la protección de los mismos.

f. Se deben aplicar controles de seguridad sobre los datos utilizados por las personas desarrolladoras o terceros en los ambientes de desarrollo y pruebas, para prevenir el acceso no autorizado a los datos confidenciales.

g. Se debe mantener el control de versiones de toda la documentación generada antes, durante y después del desarrollo, incluyendo archivos ejecutables, librerías, códigos fuentes y manuales. Además, se deben aplicar mecanismos de protección en el repositorio definido para este fin.

h. El desarrollo de software realizado por terceros, debe considerar los requisitos de seguridad establecidos por área de Informática de Gestión y el área de Sistemas.

i. Todo desarrollo de software debe considerar la identificación y clasificación de la información que será gestionada.

j. Todo sistema debe contar con un módulo para la administración de la seguridad de manera tal que los despachos y oficinas puedan gestionar sus permisos.

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

5.0 MEDICIÓN DEL CUMPLIMIENTO

El cumplimiento de este lineamiento se verificará mediante diferentes métodos, entre los que se destacan: recorridos periódicos, auditorías internas y externas, reportes de las jefaturas, o cualquier otro mecanismo definido por la Dirección de Tecnología de Información y Comunicaciones.

6.0 EXCEPCIONES

Cualquier excepción a este lineamiento debe ser aprobado previamente por Consejo Superior o quien éste designe como responsable para la aprobación del mismo.

7.0 INCUMPLIMIENTOS

Cualquier persona que labore o brinde apoyo al Poder Judicial y que no cumpla con lo aquí estipulado, queda sujeta a las sanciones disciplinarias y/o legales que los órganos correspondientes determinen. La Dirección de Tecnología de Información y Comunicaciones elaborará un informe donde se incluya un análisis de los riesgos derivados del incumplimiento, así como del posible impacto asociado.

9.0 DOCUMENTACIÓN RELACIONADA

- Normas técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República.
- Política de Seguridad de la Información.
- Reglamento del Gobierno, de la Gestión y el uso de los Servicios Tecnológicos del Poder Judicial.
- Principios de ingeniería para sistema seguro

10.0 HISTORIAL DE VERSIONES

Fecha	Revisión #	Descripción del cambio	Responsable