



**RESOLUCION EXENTA N° FC-F-00269**  
**MAT: APRUEBA POLÍTICA DE**  
**DESARROLLO SEGURO DE SOFTWARE Y**  
**SISTEMAS, POLÍTICA-SSI-A-8.25**  
**SANTIAGO, 28-04-2025**

**VISTOS:**

Lo dispuesto en la Ley N° 18.989, en particular en su Título II sobre el Fondo de Solidaridad e Inversión Social; en el DFL N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en la Resolución N° 36 de 2024, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón; en el Decreto Supremo N° 15, de 28 de abril de 2022, del Ministerio de Desarrollo Social y Familia que nombra el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social y demás antecedentes tenidos a la vista.


**CONSIDERANDO:**

- 1°. - Que, el Fondo de Solidaridad e Inversión Social, FOSIS, es un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, cuya finalidad es financiar en todo a parte planes, programas, proyectos y actividades especiales de desarrollo social, los que deberán coordinarse con los que realicen otras reparticiones del Estado.
- 2°. - Que, el FOSIS tiene como misión el “contribuir a la superación de la pobreza y vulnerabilidad social a través de estrategias que fortalezcan la cohesión social, las habilidades y capacidades de personas, familias y comunidades, con pertinencia territorial y enfoque de género”.
- 3°. - Que, resulta necesario que el FOSIS cuente con un procedimiento que tenga como objetivo el establecer y aplicar normas para el desarrollo seguro de software y sistemas del FOSIS, garantizando que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.
- 4°. - Que, por lo anteriormente señalado, mediante Memorándum DOI-274-1102531, de 14 de abril de 2025, de la Encargada de Ciberseguridad, del FOSIS Nivel Central, se solicita aprobar por acto administrativo, la Política de Desarrollo Seguro de Software y Sistemas, Política-SSI-A-8.25, Fecha emisión: 26/11/2018, Versión: 4, Fecha versión: 14/04/2025.
- 5°. - Que, teniendo presente lo expuesto precedentemente, resulta pertinente aprobar el procedimiento antes individualizado a través del presente acto administrativo.

**RESUELVO:**

**APRUEBESE** la Política de Desarrollo Seguro de Software y Sistemas, Política-SSI-A-8.25, Fecha emisión: 26/11/2018, Versión: 4, Fecha versión: 14/04/2025, cuyo texto íntegro es el siguiente:



	<b>POLÍTICA DE DESARROLLO SEGURO DE SOFTWARE Y SISTEMAS</b>	Fecha emisión: 26/11/2018
	<b>POLÍTICA-SSI-A-8.25</b>	Fecha versión: <b>14/04/2025</b>

### 1. OBJETIVO

Establecer y **aplicar** normas para el desarrollo seguro de software y sistemas del FOSIS, **garantizando que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.**

### 2. ALCANCE

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que presten servicios al FOSIS y está dentro del alcance de la Norma NCh-ISO 27001:2023 control:

- **8.25 Ciclo de vida de desarrollo seguro**

### 3. DOCUMENTOS RELACIONADOS

- [Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, sus políticas, procedimientos e instructivos.](#)
- [NCh-ISO 27001:2023 Seguridad de la Información, Ciberseguridad y protección de la privacidad – Sistema de gestión de Seguridad de la Información- Requisitos.](#)
- [Decreto N° 83, de 2004, de la Secretaría General de la Presidencia: Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad del documento electrónico.](#)
- [Guía Técnica Lineamientos para desarrollo de software División de Gobierno Digital](#)
- [Decreto 11 de 2023 establece norma técnica de calidad y funcionamiento de las plataformas electrónicas que sustentan procedimientos administrativos en los órganos de la administración del estado](#)

Elaborado por:  <b>Roxana Vercoutere Carter</b>  Encargada Ciberseguridad	Aprobado por:  <b>Cristian Salomó González</b>  Encargado de Seguridad de la Información  <b>Subdirector de Usuarios</b>
Fecha: 14/04/2025	Fecha: 14.04.2025
Documento Impreso – Copia no controlada sin timbre original	



#### 4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado(a) de Seguridad de la Información.	<ul style="list-style-type: none"> <li>• Coordinar revisiones periódicas del cumplimiento de la política.</li> <li>• Proponer nuevas prácticas de seguridad para el desarrollo de sistemas.</li> </ul>
<b>Encargado(a) de proyectos tecnológicos</b>	<ul style="list-style-type: none"> <li>• Velar por el cumplimiento de las disposiciones definidas en esta política.</li> <li>• Documentar el sistema y/o sus modificaciones.</li> <li>• Documentar los desarrollos nuevos y/o modificaciones de software, además de los resultados de comportamiento en los ambientes de Desarrollo y/o QA, se debe evidenciar el plan de pruebas, incluyendo pruebas unitarias e integrales.</li> <li>• Aplicar el procedimiento y registro de todas las actividades de "Paso a Producción".</li> </ul>
<b>Jefe(a) Tecnologías de la Información y Telecomunicaciones</b>	<ul style="list-style-type: none"> <li>• Validar y autorizar los cambios que sufran los sistemas de información.</li> <li>• Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información.</li> <li>• Disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información.</li> <li>• Velar por el soporte de los sistemas desarrollados.</li> </ul>
Gestor de compra Encargado del proyecto	<ul style="list-style-type: none"> <li>• Velar por la continuidad de las actualizaciones y requerimientos de los contratos de servicios en materias de desarrollo de software.</li> </ul>

#### 5. POLÍTICA

##### 5.1. Consideraciones generales

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguro. Para ello, se deben considerar los siguientes aspectos:

- Separar los entornos de desarrollo, prueba y producción
- Asegurar la seguridad en metodología de desarrollo de software
- Establecer directrices de codificación segura para cada lenguaje de programación usado.
- Establecer requisitos de seguridad en la fase de especificación y diseño
- Establecer controles de seguridad en proyectos de desarrollo de software
- Realizar pruebas de sistemas y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración.
- Tener repositorios seguros para código fuente y configuración.
- Mantener la seguridad en el control de versiones.
- Tener conocimientos y formación en materia de seguridad de las aplicaciones.
- Asegurar que los desarrolladores tienen la capacidad para prevenir, encontrar y corregir vulnerabilidades.
- Conocer los requisitos de licencia y las alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia.



- **En caso de desarrollos externos, obtener garantías de que el proveedor cumple con las normas de la organización para el desarrollo seguro.**
- Planificar y ejecutar el mantenimiento de los sistemas de la institución, además de pruebas de funcionamiento de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.
- estandarizar el ciclo de desarrollo de sistemas, tal como lo establece la metodología de desarrollo y mantención de sistemas definida en el FOSIS.
- establecer estándares de criterios de seguridad y de calidad en el desarrollo de sistemas.
- Toda modificación de software crítico, por parches o módulos adicionales, debe ser analizada previamente en los ambientes de desarrollo y prueba.
- planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterios de aceptación del cambio y un plan de vuelta atrás.
- Los programadores y personal de terceros no deben tener acceso a información de producción que contenga datos sensibles.
- Para propósitos de desarrollo y pruebas, los responsables deben generar sus propios datos, debiendo ser distintos a los que se encuentran en ambiente de producción.
- Un sistema desarrollado o modificado por terceras partes debe cumplir con lo establecido en esta política, incluyendo los criterios de seguridad.
- Todo desarrollo interno/externo debe estar almacenado en un repositorio que mantenga su versionamiento de código fuente<sup>[4]</sup>.
- Para cualquier desarrollo debe considerarse lo dispuesto en el procedimiento para separar ambientes de desarrollo, QA y producción.

## 5.2 Desarrollo por proveedores externos

Se debe establecer un acuerdo previo con los proveedores externos, que resguarde la propiedad intelectual<sup>[2]</sup> y asegure los niveles de confidencialidad de la información manejada en el proyecto y **velar por el cumplimiento de las políticas internas del FOSIS, principalmente, la Política de seguridad de la información para las relaciones con el proveedor.**

## 5.3 Gestión de vulnerabilidades

Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad<sup>[3]</sup> que surgen en los productos de software, que son publicadas en internet por los proveedores de tecnología asociada y proponer las medidas de mitigación al riesgo definido.

Se debe efectuar validaciones y evaluaciones periódicas de seguridad durante el ciclo de vida del **software o sistema.**

A lo menos una vez cada tres meses, el Departamento de **Tecnologías de la Información y Telecomunicaciones** debe realizar un escaneo de las aplicaciones en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas<sup>[4]</sup>. **El informe que resulte de esta revisión debe ser enviado trimestralmente al(la) Encargado(a) de ciberseguridad.**

## 5.4 Documentación

- El diccionario de datos, o repositorio de metadatos, debe mantener una descripción actualizada de las definiciones de datos.
- Si el programador incluye comentarios en el programa fuente, éstos deben ser útiles para un tercero y no divulgar información de configuración.
- Respecto a la documentación, ésta se debe:
  - a. Generar durante el ciclo de desarrollo y no postergarla hasta el final.
  - b. Revisar por los usuarios finales del sistema en desarrollo.
  - c. Actualizar si el programa cambia alguna de sus funcionalidades.



- d. Almacenar en un sitio centralizado (Servidor) administrado por el departamento de **Tecnologías de la Información y Telecomunicaciones**.

### 5.5 Evaluación de proyectos<sup>[5]</sup>

Como parte de las actividades a realizar en esta fase de un proyecto de desarrollo de un sistema de información, se debe clarificar la problemática actual, teniendo en cuenta siempre la seguridad de la información de la solución propuesta, que debe ser cubierta por el nuevo sistema.<sup>[6]</sup>

Se debe presentar una evaluación completa de costos, futuras licencias y beneficios que tendría el nuevo sistema.

En el estudio de factibilidad o anteproyecto, se debe considerar el aspecto de seguridad, el nivel de criticidad del sistema y de los controles que se deben predefinir.

#### 5.5.1. Especificación detallada de requerimientos

En el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requieren los datos y las aplicaciones que lo compongan.

Los requerimientos de seguridad deben ser compatibles con lo que se establece en las otras Políticas de Seguridad.

### 5.6. Diseño del Sistema

- El nivel de sensibilidad debe ser definido para cada elemento de datos, archivo, programa y sistema.
- Si se define utilizar cifrado de datos, debe estar definido en el estándar de cifrados<sup>[7]</sup>.
- Si se utiliza un administrador de bases de datos, se deben emplear las herramientas de seguridad que el producto provee.
- Todos los programas críticos deben incluir la generación **y almacenamiento** de registros de auditoría<sup>[8]</sup>, considerando como mínimo, la identidad del usuario que lee o escribe y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
- En la etapa de diseño se debe proyectar el rendimiento esperado de un sistema informático, con el objetivo de no sobredimensionar los recursos necesarios para el funcionamiento del Sistema (ancho de banda, RAM, recursos del servidor, etc.).

### 5.7. Codificación y Pruebas

- Todo cambio debe quedar registrado y documentado.
- No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.
- **Las pruebas del sistema deben incluir:** instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores.
- Las pruebas deben ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.
- Se debe documentar el resultado de las pruebas que son parte integrante de la solicitud de paso a producción.
- **Anterior al paso a producción, se deben realizar pruebas de seguridad, validadas por el encargado de ciberseguridad ministerial, con el fin de coordinar que las tecnologías a implementar sean compatibles, interoperables y cumplan con la normativa vigente.**
- El pase a producción debe ser autorizado por el **Jefe de Tecnologías de Información y Telecomunicaciones**, quién debe validar la presencia de todos los documentos que avalen un buen desarrollo de las aplicaciones.

### 5.8. Implementación

El **encargado o gestor del proyecto** debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.



TIC debe efectuar sintonía o ajuste (tunning) de los controles establecidos en la fase de diseño.

### 5.9. Post Implementación

Se debe revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.

### 5.10. Controles para implementar

- Se debe considerar e implementar, al menos, los siguientes controles:
  - a. Validación de datos de entrada y de salida.
  - b. Controles de procesamiento interno.
  - c. Controles criptográficos
  - d. Protección de los datos de prueba.
  - e. Segregación de acceso a datos.
  - f. Pent testing de aplicación integral con herramienta automática.
  - g. Repositorio de programas fuentes.
- En caso de vulnerar cualquiera de estos controles que puedan afectar la seguridad de la información, esto debe ser informado a través del registro de incidentes de seguridad disponible en intranet<sup>[9]</sup>.

### 5.11. Uso de Inteligencia Artificial en los desarrollos y sistemas

**Cuando se use la inteligencia artificial en cualquier desarrollo de sistema, se deben tomar las medidas para mitigar sus riesgos inherentes, para esto se debe considerar lo dispuesto en la política para el uso de Inteligencia artificial de FOSIS y tomar las siguientes consideraciones:**

#### 5.11.1. Identifique las aplicaciones de IA adecuadas:

- **Análisis de código estático y dinámico**
- **Predicción de vulnerabilidades**
- **Detección y respuesta a amenazas**
- **Pruebas de penetración automatizadas**
- **Análisis seguro de composición de software (SCA)**
- **Automatización de DevSecOps**

#### 5.11.2. Aborde los riesgos de la integración de la IA:

- **Seguridad y privacidad de los datos**
- **Seguridad del modelo**
- **Sesgo y equidad**
- **Explicabilidad y transparencia**
- **Ataques adversarios**
- **Bloqueo de proveedores**

## 6. DIFUSIÓN

La comunicación de la presente política se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se debe hacer difusión mediante los siguientes canales:

- Publicación en la intranet del FOSIS
- Correo informativo.



## 7. SANCIONES

El incumplimiento de las obligaciones emanadas de esta política será sancionado en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del FOSIS. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

## 8. REVISIÓN Y MEDICIÓN

La presente política deberá ser revisada a lo menos cada **dos** años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

## 9. CONTROL DE VERSIONES

Versión	Fecha de Aprobación	Motivo del Cambio
2	25/09/2019	Actualiza logo Modifica alcance Agrega documentos relacionados Actualiza departamentos
3	29/11/2021	Actualiza cargo jefe de informática y telecomunicaciones Referencia sobre políticas y procedimientos complementarios a la política
4	14/04/2025	<b>Actualiza cargos y normativa vigente</b>

Firmado por: Roxana Vercoutere Carter, Encargada Ciberseguridad; Cristian Salomó González, Encargado de Seguridad de la Información, Subdirector de Usuarios.

<p>[1] Ver política para el respaldo de información y software</p> <p>1 Ver política de propiedad intelectual</p> <p>[3] Ver procedimiento para la gestión de vulnerabilidades técnicas</p> <p>[4] Cada semestre, TIC realiza pruebas de Las pruebas de recuperación ante desastres (DR) son simulaciones que evalúan la capacidad de la organización para recuperar los datos y aplicaciones después de una interrupción. El objetivo de estas pruebas es garantizar que la organización pueda continuar con sus operaciones en caso de un desastre natural, un ciberataque o una falla de TI.</p> <p>[5] <a href="#">Solicitud de requerimiento del usuario(a) DRU</a></p> <p>[6] <a href="#">Ver Instructivo de seguridad de la información para la gestión de proyectos</a></p> <p>[7] Considerar lo dispuesto en la política para el uso de controles criptográficos y gestión de claves</p> <p>[8] <b>Un registro de auditoría es un registro cronológico detallado de todos los cambios que se han implementado en un sistema operativo (SO), una aplicación o un dispositivo, con el propósito de rastrear las operaciones y el uso del sistema.</b></p>
--



Los registros de auditoría se almacenan en archivos determinados y configurados por la unidad de operaciones y seguridad informática

[https://bpms.fosis.gob.cl/Login.aspx?ReturnUrl=%2FBPM\\_Mensajes\\_Crear.aspx%3F%2FDZTXLeSnEwKkYj6pAvNvGdwR%2BixdHia9G5%2FN4OG%2BTc%3D](https://bpms.fosis.gob.cl/Login.aspx?ReturnUrl=%2FBPM_Mensajes_Crear.aspx%3F%2FDZTXLeSnEwKkYj6pAvNvGdwR%2BixdHia9G5%2FN4OG%2BTc%3D)

**ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE.**

---

**NICOLAS NAVARRETE HERNANDEZ  
DIRECTOR EJECUTIVO  
FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL**

**NNH/PMD/JDG/FMZ/CSG/RVC/MCE**

**ANEXOS: SI CORRESPONDE**

**DISTRIBUCIÓN**

SUBDIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

SUBDIRECCIÓN DE USUARIOS

OFICINA DE PARTES

GESTOR: ROXANA VERCOUTERE

Fecha de Emisión: 2025-04-28 (10:51)

Válido  
indefinidamente

Código Verificación:



Nicolas Navarrete Hernandez  
Director Ejecutivo  
FOSIS

**Documento firmado con FIRMAGOB**

Verifique la validez de este documento escaneando el código QR.