1. OBJETIVO

Establecer normas para el desarrollo seguro de software nuevos y/o actualizaciones de sistemas existentes en FOSIS.

2. ALCANCE

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que presten servicios al FOSIS

Norma NCh-ISO 27001:2013 control:

- **Control 14.2.1 Política de desarrollo seguro**

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, Res. 0879/12-07-2019.
- NCh-ISO 27001:2013 Tecnología de la información – Técnicas de seguridad – 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.
- **Política de propiedad intelectual FOSIS**
- **Guía Técnica Lineamientos para desarrollo de software Ministerio Secretaría General de la Presidencia**

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad de la Información.	Coordinar revisiones periódicas del **cumplimiento de la política.** Proponer nuevas prácticas de seguridad para el desarrollo de sistemas.
Jefe Departamento de Transformación Digital.	**Velar por el cumplimiento de** las disposiciones definidas en esta política. Documentar el sistema y/o sus modificaciones. 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. Aplicar el procedimiento y registro de todas las actividades de "Paso a Producción".
Jefe Departamento de soporte y operaciones TIC	Validar y autorizar los cambios que sufran los sistemas de información. Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información. Disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información. Velar por el soporte de los sistemas desarrollados.

5. POLÍTICA

5.1. Consideraciones generales

- Se debe 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.
- Se debe estandarizar el ciclo de desarrollo de sistemas, tal como lo establece la metodología de desarrollo y mantención de sistemas definida en el Fondo de Solidaridad e Inversión Social.
- Se debe 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.
- Se deben 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.**

5.2. Desarrollo por proveedores externos

Se debe establecer un acuerdo previo con los proveedores externos, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.

5.3. Gestión de vulnerabilidades

Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que son publicadas en internet por lo 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 proyecto.

A lo menos una vez cada tres meses, **el departamento de soporte y operaciones TIC** debe realizar un escaneo de las aplicaciones en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

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 innecesaria.
- Respecto a la documentación, ésta se debe:
    - Generar durante el ciclo de desarrollo y no postergarla hasta el final.
    - Revisar por los usuarios finales del sistema en desarrollo.
    - Actualizar si el programa cambia alguna de sus funcionalidades.
    - Almacenar en un sitio centralizado (Servidor) administrado por el departamento de soporte y operaciones TIC.

5.5. Evaluación o Casos de Negocio

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.

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, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.

5.6. 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.

5.7. 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.
- 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 de registros de auditoría, 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.).

5.8. Codificación y Pruebas

- **Cuando sea necesario** modificar programas **debe quedar** registrado o documentado el cambio.
- Se deben usar técnicas de programación modular, usando lenguajes de alto nivel.
- 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.
- En lo posible, las pruebas del sistema deben incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores.
- En lo posible, 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.**
- El pase a producción debe ser autorizado por el jefe del Departamento de **soporte y operaciones TIC** en donde se debe validar la presencia de todos los documentos que avalen un buen desarrollo de las aplicaciones.

5.9. Implementación

Se 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.

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

5.10. Post Implementación

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

5.11. Controles para implementar

- Se debe considerar e implementar, al menos, los siguientes controles:
  - Validación de datos de entrada y de salida.
  - Controles de procesamiento interno.
  - Controles criptográficos
  - Protección de los datos de prueba.
  - Segregación de acceso a datos.
  - Pent testing de aplicación integral con herramienta automática.
  - Repositorio de programas fuentes.

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 de 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 tres 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
1	25/09/2019	Actualiza logo Modifica alcance Agrega documentos relacionados Actualiza departamentos