POL-SSI-14

POLÍTICA DE DESARROLLO SEGURO

PRESIDENCIA DE LA REPÚBLICA

Aprobado por: Julio Maiers Hechenleitner

Director Administrativo

NOTA DE SENSIBILIDAD Y PROPIEDAD INTELECTUAL

Tabla de Contenidos:

1. Objetivo.

Establecer las reglas para el desarrollo de sistemas de información institucionales con la finalidad de ser aplicadas por las contrapartes internas correspondientes.

2. Alcance.

El alcance de este documento aplica al desarrollo de software y sistemas realizado internamente por la Presidencia de la República.

3. Roles y Responsabilidades.

- **Director Administrativo.**
  Responsable de liderar la implantación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asignando los recursos técnicos y humanos necesarios para mantener activo dicho sistema, mediante la promulgación de políticas internas que indiquen lineamientos y las obligaciones de las personas (usuarios) de la institución.

- **Integrantes del Comité de Seguridad de la Información.**
  Responsables de apoyar y gestionar la implementación de los requisitos de seguridad de la información del SGSI para el correcto y adecuado uso de los activos de información de la Institución.

- **Encargado de Seguridad de la Información.**
  Responsable de supervisar y coordinar las actividades de monitoreo, control y evaluación del SGSI de la institución para el cumplimiento de los requisitos de seguridad de la información.

- **Encargado de Desarrollo.**
  Responsable de implementar las actividades y controles necesarios para el desarrollo seguro de software y sistemas de la institución.

- **Coordinadores del SGSI**
  Responsables de gestionar el cumplimiento de los requisitos de seguridad del SGSI vinculados a su Departamento a través de la correcta aplicación de las políticas y procedimientos asociados.

4. Definiciones (contenido).

La Dirección Administrativa se asegura establecer reglas que permitan realizar el desarrollo seguro de sistemas de información, en virtud de generar un servicio, arquitectura, software y sistemas seguros para los activos de información relacionados con este proceso.

Para el cumplimiento de lo anterior, el Departamento de TIC debe considerar las siguientes definiciones:

a) Definir, implementar y revisar la separación de ambientes destinados al desarrollo de software y sistemas, bajo la siguiente estructura: (1) ambiente de desarrollo, (2) ambiente de pruebas, (3) ambiente productivo. Los dos últimos ambientes (pruebas y productivo) deben tener las mismas características técnicas para asegurar la correcta implementación de controles de seguridad y pruebas;

b) Disponer de una metodología para el desarrollo y mantención de software y sistemas de manera segura, considerando la incorporación de controles de seguridad de la información en el desarrollo de sistemas, en cumplimiento con la Guía de Desarrollo de Software para el Estado;

c) Establecer los requisitos de seguridad que se exigirán en las diferentes etapas del diseño de los sistemas, mediante el uso de procedimientos relacionados (Ver PRO – SSI – 14 – Adquisición, desarrollo y mantenimiento del sistema);

d) Para cada proyecto de desarrollo de software o sistema, definir los puntos de verificación de seguridad que se utilizarán en los diferentes hitos de cada proyecto;

e) Considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha, planificando y documentando las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-implementación, criterio de aceptación del cambio y plan de vuelta atrás;

f) Asegurar que los software y sistemas construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros;

g) Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de software y sistemas que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación;

h) Remover todas las funcionalidades y archivos que no sean necesarios para software y sistemas, previo a la puesta en producción y prevenir la revelación de la estructura de directorios de los sistemas tecnológicos construidos;

i) Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado, asegurando los encabezados de respuestas http en servidores;

j) Desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura;

k) Proteger el código fuente de software y sistemas desarrollados, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

5. Periodicidad de Evaluación y Revisión.

Los lineamientos y alcances contenidos en esta política son susceptibles de mejorar continuamente, por lo tanto, son factibles de someter a modificaciones, actualizaciones y cambios periódicos tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que la institución se encuentre.

Sin perjuicio de lo anterior, se establece que la periodicidad ordinaria de revisión de esta política es **anual.**

6. Difusión.

La presente política y sus lineamientos estratégicos están disponibles al personal bajo el control de la Presidencia de la República y terceros, según corresponda.

El mecanismo de difusión de esta política es:

- Publicación en la Intranet institucional.
- Publicación en el Portal de transparencia institucional.

7. Control de Cambios.

Versión	Fecha	Principales revisiones y/o modificaciones	Nº de revisión	Elaborado por	Revisado por	Aprobado por (responsable del documento)
01	03.09.2012	Versión inicial. (firma y timbre director administrativo)	01	Encargado de Seguridad de la Información	Jefe de Departamento TIC	Director Administrativo
02	26.12.2016	-Actualización de documento según requerimientos de NCh-ISO 27001:2013. -El presente documento se aprueba bajo Resolución Exenta N° 2487, con fecha 26.12.2016.	02	Encargado de Seguridad de la Información	Jefe de Departamento TIC	Director Administrativo
03	07.11.2017	-Se actualiza codificación de este documento, se reemplaza "POL-TIC-07" por "POL-SSI-08", producto de la nueva forma de identificar los documentos. (todas las páginas, encabezado del documento). -Se incorporan las tablas "Objetivo y Productos estratégicos y Procesos Críticos en ámbito de aplicación del PMG-SSI PRESIDENCIA)" y "Alcance de Dominios y Controles de Seguridad de la Información asociados a este documento" (página 5, sección 3.-Alcance o Ámbito de Aplicación. - Se incorpora en página 4 la sección 5.- Materias que aborda el documento. - Se posiciona al final del documento la tabla de Historial de versiones (control de cambios) incorporando en columna "Principales Modificaciones" el texto (Página / Sección) y se crea una nueva columna denominada "Motivo del Cambio", (página 11 / sección 10.-Historial de versiones (control de cambios). -El presente documento se aprueba bajo Resolución Exenta N° 2078, con fecha 07.11.2017.	03	Encargado de Seguridad de la Información	Jefe de Departamento TIC	Director Administrativo
04	19.11.2018	- Sección alcance. -El presente documento se aprueba bajo Resolución Exenta N° 1998, con fecha 19.11.2018.	04	Encargado de Seguridad de la Información	Jefe de Departamento TIC	Director Administrativo
05	13.11.2019	-Se ajusta nombre codificación y contenido de política según los requisitos del control NChISO27001 A.14.2.1 y un nuevo orden establecido para el SGSI institucional. -El presente documento se aprueba bajo firma electrónica del Director Administrativo.	05	Encargado de Seguridad de la Información	Jefatura Depto. de TIC.	Director Administrativo