



PS-NC-002


POLITICA DESARROLLO DE SISTEMAS

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v02 – Octubre del 2019


	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Encargado PMG SSI	Octubre 2019	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2019	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2019	



POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 2 de 8

Contenido

1	PROPOSITO	3
2	ALCANCE O AMBITO DE APLICACIÓN	3
3	MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS	3
4	ROLES Y RESPONSABILIDADES	4
5	MATERIAS QUE ABORDA.....	4
6	DIRECTRICES DE LA POLÍTICA.....	5
6.1	Cumplimiento de la legislación	5
6.2	Definiciones asociadas a la Seguridad de las Telecomunicaciones	5
6.3	Lineamientos generales	5
6.4	Análisis previo del Sistema de Información.....	5
6.5	Diseño del Sistema de Información.....	5
6.6	Desarrollo y Testing.	6
6.7	Marcha Blanca y Producción	7
6.8	Separación de Ambientes.....	7
6.9	Adquisición de Sistemas a Terceros	8
7	MECANISMO DE DIFUSIÓN.	8
8	PERÍODO DE REVISIÓN.	8
9	EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA	8
10	HISTORIAL Y CONTROL DE VERSIONES	8

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 3 de 8

1 PROPOSITO

Esta Política de Desarrollo de Sistemas, establece los lineamientos para garantizar la seguridad en los productos de software para las instituciones del Sector Salud.

Define las directrices y requisitos que deben estar presentes en los desarrollos tanto internos como externos de la institución, considerándolas en cada una de las etapas de desarrollo, controlando los ambientes de trabajo en desarrollo, testing y producción.

2 ALCANCE O AMBITO DE APLICACIÓN

La presente política se aplica a todos los sistemas de información desarrollados y/o actualizados en el Minsal, ya sea en forma interna como por empresas o profesionales externos contratados para tales efectos.


Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Seguridad de las operaciones	A.12.01.04	Separación de los ambientes de desarrollo, prueba y operacionales
	A.12.05.01	Instalación del software en sistemas operacionales
Adquisición, desarrollo y mantenimiento del sistema	A.14.02.01	Política de desarrollo seguro
	A.14.02.02	Procedimientos de control de cambios del sistema
	A.14.02.06	Entorno de desarrollo seguro
	A.14.02.08	Prueba de seguridad del sistema
	A.14.02.09	Prueba de aprobación del sistema

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
 - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 4 de 8

- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
 - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
 - Leyes relacionadas

- **Documentos Relacionados**

- Procedimiento de desarrollo seguro.

4 ROLES Y RESPONSABILIDADES

- **Jefe Departamento TIC**

- Debe disponer los controles y reglas de control de acceso.

- **Encargado de Seguridad de la Información / Encargado de Ciberseguridad.**

- Coordinar revisiones periódicas de seguridad en los sistemas de producción.
- Proponer nuevas prácticas de seguridad para el desarrollo de sistemas.

- **Operaciones TIC (Soporte).**

- Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información.

- **Operaciones TIC (desarrollo de sistemas) / Áreas de Negocio que cuenten con equipos de desarrollo de sistemas.**


- Cumplir con las disposiciones definidas en esta política.
- Documentar el Sistema y/o sus modificaciones.

- **Operaciones TIC (Infraestructura).**

- Disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información.

5 MATERIAS QUE ABORDA.

- Separación de los ambientes de desarrollo, prueba y operacionales.
- Política de desarrollo seguro.
- Entorno de desarrollo seguro.
- Prueba de seguridad del sistema.
- Prueba de aprobación del sistema.

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 5 de 8

6 DIRECTRICES DE LA POLÍTICA

6.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento “Normativa del Sistema de Gestión de Seguridad de la Información”.

6.2 Definiciones asociadas a la Seguridad de las Telecomunicaciones

Las siguientes definiciones son específicas para el ámbito de seguridad en el desarrollo de sistemas:

- Entorno pre-productivo, asociado a los ambientes de trabajo de Desarrollo y Testing.

6.3 Lineamientos generales


- Se deben estandarizar los criterios de seguridad y de calidad a ser considerados durante cada fase del ciclo de desarrollo de los sistemas.
- Todo sistema desarrollado en la Institución debe cumplir con las disposiciones de esta política.
- En el contexto de esta política, se define sistemas críticos como aquellos componentes de software desarrollados interna o externamente, que son parte sensible de Institución.
- El desarrollo de trabajo externo debe seguir las mismas etapas definidas en este documento.

6.4 Análisis previo del Sistema de Información.

- Como parte de la fase de evaluación se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.
- En el estudio de factibilidad, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.
- Se deben recolectar y autorizar debidamente los requerimientos de los usuarios para realizar el documento inicial para el desarrollo de este. En esta etapa es importante la participación del jefe de proyecto y usuario solicitante.

6.5 Diseño del Sistema de Información.


- En el diseño de un proyecto, se deben considerar: el diseño de presentación, diseño de arquitectura, diseño de Base de datos y lógica del sistema.
 - Diseño de presentación, este permitirá determinar como el usuario solicitante verá el sistema cuando esté finalizado.

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00 Página 6 de 8

- Diseño de arquitectura, este permitirá indicar que tipo de proyecto (web, escritorio, webservices, móvil), su interacción con otros desarrollos, definiendo el lenguaje en que se desarrollará.
- Diseño base de datos, se debe encargarse de generar el diseño lógico y conceptual del modelo del negocio que permita el mejor desarrollo del proyecto.
- Se deben coordinar la participación de Jefe de Proyecto, Encargado de la mantención de la base de datos, Encargado de plataforma de soporte de las aplicaciones para realizar los aportes necesarios para realizar el proyecto, este debe ser finalizado con el levantamiento final de los requerimientos que deben quedar en el documento de levantamiento de requerimientos.
- Los datos que deben contener un registro de auditoría son: la identidad del usuario creador y modificador, fecha y hora del evento creador y modificador.
- Los registros de auditoría deben ser protegidos contra el acceso y la manipulación no autorizada.

6.6 Desarrollo y Testing.

- Existe prohibición de:
 - Escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos) usando infraestructura de la Institución.
 - Incluir funciones u operaciones no documentadas o no autorizadas en los programas.
 - Modificar programas sin que quede registrado o documentado el cambio.
- La generación de código fuente debe quedar en el repositorio correspondiente para tener la trazabilidad de las modificaciones.
- El acceso a código fuente de los distintos sistemas debe estar protegido para acceder solo con las contraseñas asignadas.
- Para consultores externos se le debe dar acceso al código solo en el periodo que dure el proyecto.
- Toda empresa externa que trabaje con códigos de sistemas críticos debe de firmar una carta de confidencialidad.
- El desarrollo de los sistemas se realiza en un ambiente local, utilizando datos de base de datos propias de desarrollo, distintas a las de producción.
- El desarrollo se basa en el documento de levantamiento de requerimiento.
- Deben considerarse al menos 2 tipos de testing, el que realiza el equipo de testing; y el del usuario solicitante o acreditación usuaria.
- Las pruebas del sistema deben incluir: pruebas de integración (instalación, almacenamiento, configuración, seguridad, recuperación ante errores), pruebas funcionales y de rendimiento. Estos quedan registrados en el documento plan de prueba.
- El control de acceso usado en el ambiente de testing debe ser tan estricto como el usado en el ambiente de producción.
- Los usuarios solicitantes acceden al ambiente de testing solo tienen acceso a lectura de la información.
- La copia de datos desde ambiente de producción al ambiente de testing se realiza una vez que la etapa de la marcha blanca se finalice.

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 7 de 8


- Los sistemas críticos deben incluir la validación de los datos de entrada, para asegurar un correcto procesamiento.
- Los sistemas críticos deben incluir controles de validación de los datos de salida, para asegurar que el procesamiento ejecutado haya sido correcto.
- Los sistemas críticos que interactúen con otros deben incluir controles para asegurar la integridad de los mensajes intercambiados.

6.7 Marcha Blanca y Producción

- El paso a producción del proyecto es autorizado por el usuario solicitante cuando termina el testing a través de correo electrónico.
- Según el proyecto se define los tiempos de la marcha blanca.
- Se deben revisar y auditar los controles de seguridad definidos en la etapa de diseño.
- El equipo de desarrollo debe revisar y auditar sus propios sistemas antes de pasar a la etapa de pruebas formales.
- El equipo de pruebas (“testing”), debe revisar y auditar los controles de seguridad, según las especificaciones generadas en la etapa de diseño.
- Si hay modificaciones al proyecto se debe comenzar el ciclo nuevamente, comenzando con el levantamiento de requerimientos.
- Todo traspaso a producción se debe hacer durante períodos de baja carga de trabajo, debidamente coordinados con el área dueña del sistema.

6.8 Separación de Ambientes

- Deben existir entornos de trabajo separados para desarrollo, testing y producción, considerando:
 - Separación de red: segmentos de red, distintos IP.
 - Separación de la versión del sistema.
 - Separación de la base de datos.
 - Separación de roles, con roles en los distintos ambientes.
- A no ser que sea bajo circunstancias excepcionales, no se deberían realizar pruebas en los sistemas productivos (estas deben ser aprobadas por el Encargado de Seguridad / Ciberseguridad).
- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían estar accesibles desde los sistemas operacionales cuando no sea necesario.
- Los usuarios deben utilizar distintos perfiles de usuario para los sistemas operacionales y de prueba y se deberían mostrar menús para mostrar mensajes de identificación adecuados para reducir el riesgo adicional.
- Toda modificación de software crítico por parches o módulos adicionales, debe ser analizada previamente en los ambientes de desarrollo y prueba.
- Se debe planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterio de aceptación del cambio y un plan de vuelta atrás.

POLITICA DESARROLLO DE SISTEMAS			
	Sistema de Gestión de Seguridad de la Información – Nivel Central		
	MINISTERIO DE SALUD	ID: PS-NC-002	Versión: 02.00
			Página 8 de 8

6.9 Adquisición de Sistemas a Terceros

- Se debe establecer un acuerdo previo y formal con instituciones o empresas externas, que resguarde la propiedad intelectual, uso de datos y asegure los niveles de confidencialidad de la información manejada en el proyecto.
- Además, se deberán incluir las responsabilidades de terceros en la gestión de incidentes de seguridad.
- Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.
- El proceso de adquisición del sistema debe ser formal y cumplir con las disposiciones de seguridad descritas en esta política.

7 MECANISMO DE DIFUSIÓN.

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

- Publicación en la intranet de Minsal <http://isalud.minsal.cl/>
- Correo informativo.

8 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Agosto 2014	Todas	Creación del Documento
02	Octubre 2019	Todas	Cambio de formato de documento. Se actualizan las referencias normativas. Se actualizan todos los puntos de la política.