POLÍTICA DE DESARROLLO, MANTENCIÓN Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

Versión 1.0

MINISTERIO DE OBRAS PÚBLICAS

ELABORADO POR:	**REVISADO POR:**	**APROBADO:**
Dirección General de Obras Públicas **FECHA: 9/09/2012**	Jefe Subdirección de Informática y Telecomunicaciones Oficial de Seguridad Información MOP **FECHA: 14/11/2012**	Comité de Seguridad de la Información **FECHA: 11/12/2012**

Índice

Control de Versión

REVISIÓN	Numeral del procedimiento	**MODIFICACIÓN REALIZADA**	**Nombre y Firma de quien autoriza**	**FECHA DEL CAMBIO**

1. Introducción

La presente política, se enmarca dentro de la Política General de Seguridad de la Información para el Ministerio de Obras Públicas (MOP), contenida en ORD N° 3082 del 12 de Diciembre del 2011, y de las recomendaciones de seguridad dadas en el Decreto Supremo MINSEGPRES N° 83 (DS 83), de 23 de Junio del 2004.

En particular este documento, junto con la norma respectiva, define el objetivo y alcance de la Política de Desarrollo, Mantención y Adquisición de Sistemas de Información del MOP.

2. Objetivo General

Definir las medidas y controles para la inclusión de inspecciones de seguridad en el proceso de construcción, mantención, adquisición y explotación de sistemas de información.

3. Objetivos Específicos

Definir los resguardos que deben aplicarse para garantizar la seguridad de los sistemas de información y de los procesos de construcción, mantención o adquisición de éstos. Así como establece las normas y documentación que deben respaldar los procesos de construcción, pruebas, mantención y explotación de los sistemas de información.

4. Alcance

Están dentro del alcance de esta política, todas las construcciones o adquisiciones de sistemas de información del Ministerio de Obras Publicas. Están también, dentro del alcance de esta política, los procesos y servicios de interoperación electrónica, entre el MOP y otras entidades públicas y privadas.

5. Destinatarios

Todos los funcionarios que son responsables de la definición, planificación, construcción, mantención y adquisición de sistemas de información en el Ministerio de Obras Públicas.

6. Política de Desarrollo, Mantención y Adquisición de Sistemas de Información

6.1. Responsabilidades

Jefe Subdirección de Informática y Telecomunicaciones

6.1.1. Definir y dictar las políticas, estándares en tecnologías, seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa legal.

6.1.2. El Jefe de la Subdirección de Informática y Telecomunicaciones, en conjunto con la Unidad de Seguridad de la Información, son los responsables de la seguridad de los sistemas de información (seguridad informática) del Ministerio de Obras Públicas.

6.1.3. Informar por escrito y en forma oportuna, a todos los proveedores de servicios externos, respecto de cambios en los responsables de la Subdirección de Informática y Telecomunicaciones relacionados con la gestión y administración de los servicios contratados.

Jefe Unidad de Seguridad de la Información

6.1.4. El Jefe de la Unidad de Seguridad de la Información, en conjunto con el propietario, dueño o responsable del o los sistemas de información, son los responsables de definir el nivel de criticidad del sistema de información, y de identificar los controles de seguridad a aplicar para resguardarlos.

6.1.5. Revisar, aprobar (o rechazar) procesos y controles tendientes a mitigar, eliminar, o transferir los riesgos relacionados con la construcción, mantención y adquisición de sistemas de información, y según corresponda, definir procedimientos para ello.

6.1.6. Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para la construcción, mantención, y adquisición de sistemas de información.

Jefe Unidad de Desarrollo y Mantención de Sistemas de Información

6.1.7. El Jefe de la Unidad de Desarrollo y Mantención de Sistemas de Información, tienen la responsabilidad de definir las normas, procedimientos y controles que permitan asegurar que los procesos de construcción y mantención de sistemas de información se apliquen los controles necesarios para la seguridad de la información de los mismos, tales como:

a) Metodología de análisis
b) Construcción de pruebas unitarias y de integración
c) Administración de sistemas
d) Administración de bases de datos
e) Documentación
f) Sistema de gestión de código

6.1.8. El Jefe de la Unidad de Desarrollo y Mantención de Sistemas de Información, es responsable de promover y verificar el cumplimiento de las políticas de seguridad que se señalan en este documento.

Jefe Unidad de Operaciones

6.1.9. El jefe de la Unidad de Operaciones, es el responsable de implementar, mantener, difundir y disponer los mecanismos de seguridad nativos, propios de las plataformas e infraestructura, con el fin de que estos sean utilizados por las aplicaciones que serán desarrolladas para operar sobre estas plataformas.

Jefe Unidad de Servicios de Negocios

6.1.10. El Jefe de la Unidad de Servicios de Negocios, es responsable de gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de la información y comunicaciones (TIC).

6.1.11. El Jefe de la Unidad de Servicios de Negocios, deberá contar con normas orientadas a la definición, especificación y planificación de soluciones de negocios.

6.1.12. El Jefe de la Unidad de Servicios de Negocios en conjunto con el Jefe de la Unidad de Seguridad de la Información, son responsable de especificar, verificar y validar los requerimientos de seguridad que deben cumplir los paquetes de software ofertados en el mercado, independiente de cómo se realiza la adquisición por parte del Ministerio.

6.1.13. El Jefe de la Unidad de Servicios de Negocios, es responsable de promover y verificar el cumplimiento de las políticas de seguridad que se señalan en este documento.

6.2. Proceso de Construcción/Mantención de sistemas de información

6.2.1. El proceso de construcción y/o mantención de sistemas de información, debe contar con normas de programación, versionamiento, documentación y pruebas para cada etapa del ciclo de vida: construcción, pruebas, explotación.

6.2.2. El ciclo de vida de la construcción y/o mantención de sistemas de información debe incluir procedimientos de pruebas funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad.

6.2.3. El proceso de construcción y/o mantención de sistemas, así como los procesos de pruebas, deben efectuarse en ambientes dispuestos para ello.

6.2.4. Los sistemas que inter operen o intercambien datos, con otros sistemas o base de datos, pertenecientes al MOP u otro Ministerio, deben contar con controles de seguridad en ambos extremos de la comunicación.

6.2.5. La responsabilidad del proceso de construcción y/o mantención de sistemas, en particular la programación (codificación), debe tener siempre dos o más responsables de forma que no se detenga el proceso en periodos de vacaciones, licencias médicas o permisos laborales. Es decir, no debe depender una sola persona.

6.2.6. El proceso de construcción y/o mantención de sistemas de información tercerizados deben cumplir con esta política y con las normas que dicte la Unidad de Seguridad de la Información a este respecto.

6.3. Documentación de sistemas de información

6.3.1. La documentación de los sistemas de información debe obedecer a los lineamientos de documentación de sistemas adoptado por el MOP definido en una norma específica dictada por la unidad de “Servicios de Negocios”. Excepciones a esta política, son la adquisición de software empaquetado.

6.3.2. Toda la documentación asociada al ciclo de construcción y/o mantención de sistemas de información debe tener procedimientos de control de versionamiento.

6.3.3. El acceso a la documentación de sistemas de información, bibliotecas de códigos fuentes y programas ejecutables, debe estar restringida sólo a funcionarios autorizados. La excepción a esta política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios del o los sistemas de información.

6.4. Especificación de arquitectura de sistemas de información

6.4.1. La arquitectura de los sistemas de información debe obedecer a los lineamientos de arquitectura de sistemas adoptado por el MOP definidos en las normas de programación que dicte de la Subdirección de Informática y Telecomunicaciones.

6.5. Especificación de requerimientos de seguridad

6.5.1. Para la construcción de nuevos sistemas de información o mejoras a los existentes, se debe especificar los controles de seguridad desde la etapa de levantamiento de requerimientos, tales como encriptación de claves, de mensajes, de configuración; auditoria de trazabilidad; entre otros.

6.5.2. En la identificación de controles de seguridad deben participar las áreas de negocio que serán usuarios del sistema de información en construcción o proceso de mantención.

6.5.3. El diseño e implementación de controles de seguridad, deben ser preferentemente de tipo automático, evitando procesos o intervención manuales. Las excepciones deben ser aprobadas por el Jefe de la Unidad de Seguridad de la Información.

6.5.4. En la etapa de diseño, debe considerarse los procedimientos necesarios para realizar revisiones periódicas de contenidos de campos, registros, tablas (de datos), o archivos considerados sensibles, frecuencia de los respaldos y tiempos de retención de estos, y procesos de depuración (limpieza de datos, indexaciones, u otros procesos relacionados con optimización y rendimiento)

6.5.5. Se puede emplear datos de prueba extraídos desde las bases de datos de los sistemas en producción, pero sólo deben ser empleadas dentro de las instalaciones del MOP. Excepciones a esta política, deben ser autorizadas por el dueño de la información, o en su defecto la Unidad de Auditoria Ministerial y se deberá elaborar y formalizar un Convenio de Confidencialidad por parte de terceros.

6.5.6. El acceso a las bases de datos de construcción, prueba y producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). Jamás en la etapa de construcción y/o prueba se debe dar acceso a los datos de producción.

6.6. Validación de datos de entrada y salida

6.6.1. En términos generales, todo sistema que considere transformación de datos de entrada debe ser diseñada y construida considerando controles de integridad de éstos.

6.6.2. Los sistemas que se construyan en la Unidad de "Desarrollo y Mantención de Sistemas de Información" del MOP o por proveedores, y aquellos sistemas "paquetizados" que se adquieran, deben contemplar funcionalidades que permita acceder tanto a los registros de auditoría como a los registros de trazabilidad.

6.6.3. Cuando un sistema tenga previsto el envío de datos (interoperabilidad) que contengan información clasificada como reservada, se debe implementar mecanismos de cifrado de los datos.

6.7. Firma digital y de encriptación

6.7.1. El dueño o propietario de la Información, en conjunto con el Jefe de la Unidad de Seguridad de la Información, evaluarán la necesidad de usar y aplicar tecnologías de encriptación para proteger información, o de tecnologías de firma digital para firmar documentos electrónicos.

6.7.2. Se usará firma digital avanzada, sólo cuando se trate de documentos con carácter de instrumento público.

6.7.3. El proveedor de firma electrónica avanzada deberá ser una Entidad Certificadora con registro vigente, de acuerdo a lo establecido en la Ley 19.799 del Ministerio de Economía, Fomento y Reconstrucción.

6.8. Administración de claves

6.8.1. La administración de cuentas y contraseñas de acceso a los sistemas de información, debe ser centralizada. Excepciones a esta política deben ser justificadas por la unidad de "Desarrollo y Mantención de Sistemas de Información", y autorizadas por el Jefe la Subdirección de Informática de Telecomunicaciones.

6.8.2. El mecanismo de autenticación de usuarios del MOP debe estar basado en una estructura de arboles jerárquicos. Excepciones a esta política deben estar autorizadas por el Jefe de la Subdirección de Informática de Telecomunicaciones.

6.8.3. La generación de códigos de cuentas y contraseñas de acceso de los usuarios a los sistemas de información, deben asegurar, a lo menos:

a) Que los códigos de cuentas sean únicos.

b) Que la generación de contraseñas cumpla al menos con atributos tales como: largo mínimo, sean alfanuméricas, no repetibles, renovables periódicamente, y que se fuerce su cambio por el involucrado (usuario) cuando se use por primera vez.

6.8.4. El mecanismo o procedimiento de creación de grupos de usuarios, perfiles o privilegios, entre otros aspectos, deben preferentemente ser administrado en cada sistema de información. Excepciones a esta política deben ser autorizadas por el Jefe la Subdirección de Informática de Telecomunicaciones.

6.8.5. La solicitud de códigos de cuentas de acceso a los sistemas de información debe efectuarse según se establece en la Política de Control de Acceso.

6.9. Control de versiones

6.9.1. Toda la documentación, archivos ejecutable, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, debe estar bajo procedimientos de control de cambios y de versionamiento.

6.9.2. La Unidad de Operaciones debe mantener un registro actualizado de todos los sistemas en explotación, con datos respecto de versión, fecha de última compilación, responsable(s) de su mantención y soporte.

6.10. Cambios en la plataforma operativa

6.10.1. Previo a cualquier cambio, actualización, o reconfiguración, planificada, en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, la Unidad de Desarrollo y Mantención de Sistemas, debe efectuar un análisis y emitir un informe técnico que evalué los impactos y riesgos que puedan generar estos cambios.

6.11. Adquisición de paquetes de software

6.11.1. En el proceso de análisis y adquisición de paquetes de software a terceros, deben considerarse aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente eventuales cambios o modificaciones para su implantación en el MOP.

6.11.2. Las modificaciones a los paquetes de software o sistemas adquiridos a terceros, que surjan producto de su explotación y tengan relación can las seguridad de la

información, deben ser aprobados por el Jefe de la Unidad de Seguridad de la Información.

6.11.3. Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los funcionarios del MOP, del cual no se disponga de su respectiva licencia que lo autorice.

6.11.4. La instalación de paquetes de software que son denominados "OPEN" deben ser autorizados por el jefe de la Subdirección de Informática y Telecomunicaciones con el objeto de validar si están dentro de los lineamentos de herramientas de software utilizados por el MOP.

6.12. Capacitación

6.12.1. La puesta en producción de los Sistemas de Información, sean éstos construidos internamente o adquiridos a terceros, deben siempre considerar la realización de actividades de capacitación dirigida a Usuarios Finales, Administradores de Plataforma y de la Mesa de Ayuda.

7. Encargados de provisión de Servicios de Desarrollo, Mantención y Adquisición de Sistemas de Información en Direcciones dependientes del MOP

7.1.1. Aquellas Direcciones que cuenten con unidades o áreas de provisión de servicios de desarrollo, mantención y adquisición de sistemas de información tienen la obligación de cumplir con lo dictaminado en política.

8. Difusión de la Política de Desarrollo, Mantención y Adquisición de Sistemas de Información

El Director General de la Dirección General de Obras Publicas, es responsable de publicar y difundir la Política de Desarrollo, Mantención y Adquisición de Sistemas de Información.

GLOSARIO DE TÉRMINOS

Activo de Información

Personas, Sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos de negocio del Ministerio de Obras Públicas o sus Servicios dependientes.

Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los activos de información.

Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

Evento de seguridad de la información.

Ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de la seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente a la seguridad.

Incidente de Seguridad

Un incidente de seguridad es uno o varios eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Seguridad de los Activos de Información

Es proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la institución.

Dueño o Responsable de Activo de Información

El la persona designada como responsable de la integridad, confidencialidad y disponibilidad de un activo de información.