INSTRUCTIVO PARA LA SEPARACIÓN DE AMBIENTES – CONTROL DE CAMBIOS Y PASO A PRODUCCIÓN

INS-SSI-14.1 v1.0

SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Jaime Gonzalez	Encargado Unidad de TIC		27/12/2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		27/12/2017

TABLA DE CONTENIDO

Nota de equidad de género:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

1. OBJETIVOS DEL INSTRUCTIVO

Los objetivos generales del Instructivo de Seguridad para la Separación de Ambientes - Control de Cambios y Paso a Producción, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Normar en que los ambientes para desarrollo, prueba y operación, se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.
- Normar las acciones de Control de Cambios y Paso a Producción.
- Cumplir con el Procedimiento Recepción de Software de Terceros.

2. CONTEXTO O ÁMBITO DE APLICACIÓN

Este instructivo para la Separación de Ambientes - Control de Cambios y Paso a Producción aplica a todo el personal de la Subsecretaría de Transportes y sus Programas dependientes sean de planta, contrata o a honorarios, y externos que presten servicios a ella, e involucra a las visitas y a todos sus instalaciones, recursos y activos de información.

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:

Dominios y Controles de Seguridad relacionados	
A.12	Dominio: Seguridad de las Operaciones
A.12.01.02	Gestión de Cambios
A.12.01.04	Separación de los ambientes de desarrollo, prueba y operacionales
A.12.05.01	Instalación del software en sistemas operacionales
A.13	Dominio: Seguridad en las Telecomunicaciones
A.13.01.03	Separación en las redes
A.14	Dominio: Adquisición, desarrollo y mantenimiento del sistema
A.14.02.01	Política de desarrollo seguro
A.14.02.02	Procedimientos de control de cambios
A.14.02.05	Principios de ingeniería de sistema seguro
A.14.02.07	Desarrollo tercerizado
A.14.02.08	Prueba de seguridad del sistema
A.14.02.09	Prueba de aprobación del sistema

En cuanto al ámbito institucional de aplicación de este instructivo, corresponde a los siguientes objetivos y productos estratégicos del formulario A1 relacionados con procesos críticos que corresponden al alcance declarado del Sistema de Seguridad de la Información de SUBSECRETARÍA DE TRANSPORTE:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico SUBSECRETARÍA DE TRANSPORTE	Producto Estratégico A1	Proceso crítico protegido

(1) Disminuir fallecidos por accidentes de tránsito. (2) Desarrollar planes y estudios que permiten definir políticas y normativas en los temas relevantes a transporte de carga.	(1) Regulación que rige el transporte	Políticas y normas que rigen el transporte.
(3) Mejorar las condiciones para la operación e integración del Transporte Público a través de infraestructura prioritaria, con foco inicial en la mejora de los tiempos de viaje. (4) Diseñar sistemas de transportes que respondan a las principales necesidades multimodales de las personas, priorizando los modos más eficientes y sustentables y mejorando la convivencia de usuarios de los distintos modos. (6) Velar por la accesibilidad, calidad, seguridad e impacto ambiental que entregan los servicios de transporte terrestre y otros modos.	(5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público.	Transporte Público Regional.

3. ROLES Y RESPONSABILIDADES

- **El Encargado de Seguridad de la Información (ESI)**
  - Es responsable de la elaboración del presente instructivo, de su actualización y velar por el cumplimiento de sus disposiciones.

- **El Encargado de la Unidad de TIC**
  - Es responsable de supervisar la implementación del presente instructivo.

- **Área de Proyectos.**
  - Cumplir con las disposiciones de este instructivo para todo sistema desarrollado para la Subsecretaría.
  - Mantener vigente el conjunto de estándares de diseño que consideran aspectos de seguridad para los nuevos sistemas.

- **Encargado del área de Proyectos.**
  - Autorizar, validar y documentar los requerimientos funcionales y de seguridad.
  - Tanto para desarrollos externos como consultores, vela por el cumplimiento de los hitos comprometidos.

- **Jefe de proyectos**
  - Encargado del proyecto de desarrollo del sistema o de la adquisición e implantación del software.
  - Coordinar los proyectos desarrollados por el área y los desarrollados por terceros (externos).
  - Recibir levantamiento de los requerimientos del negocio realizados por el analista.
  - Gestionar la instalación en ambiente de desarrollo.

- Solicitar paso a ambiente de pruebas (QA).
- Solicitar Paso a Producción.
- Controlar y dar seguimiento al proyecto en las etapas de desarrollo.
- Entregar el sistema implementado al usuario solicitante junto al manual de uso respectivo
- Concluir el proceso con la verificación del usuario solicitante.

- **Ingeniero de sistemas del área de Infraestructura / Unidad TIC**
  - Revisar y planificar configuración de ambientes.
  - Ejecutar Creación de Ambientes.
  - Instalar en ambiente de Pruebas (QA).

- **Proveedor de desarrollo tercerizado**
  - Instalar sistema en ambiente de desarrollo.
  - Ejecutar Plan de Pruebas en Desarrollo y QA.
  - Realizar ajustes post pruebas.

- **Cliente Lider**
  - Ejecutar Plan de Pruebas en QA
  - Entregar aceptación del sistema

- **Desarrollador**
  - Procesar los requerimientos del analista elaborando el diseño del sistema utilizando los estándares establecidos.
  - Desarrollar los requerimientos entregados por el jefe de proyecto.
  - Redactar el manual correspondiente.

4. MATERIAS QUE ABORDA

El presente instructivo aborda las actividades de Seguridad en las Sistemas de Información, en tópicos de:

- Lineamientos de desarrollo seguro interno y tercerizado
- Separación de los ambientes de desarrollo, prueba y Producción
- Entorno de Desarrollo y Testing.
- Entorno de Producción
- Segregación de redes
- Control de cambios
- Instalación del software en sistemas operacionales
- Principios de ingeniería de sistema seguro
- Prueba de seguridad del sistema
- Prueba de aprobación del sistema

5. MODO DE OPERACIÓN

5.1 Lineamientos de desarrollo seguro interno y tercerizado

- Para todo proyecto interno o externo (tercerizado) de desarrollo, así como para la adquisición de software y sus actividades de mantención, se deben resguardar los lineamientos de Seguridad de la Información, plasmados en la Política de Seguridad en los Sistemas de Información y el presente instructivo.
- Todo proyecto de mediana envergadura o superior, o que pueda afectar la continuidad operacional de los procesos que soporte, debe formalizar su adherencia y cumplimiento a los requerimientos de la Política arriba señalada y del presente instructivo, generado por mal por el Jefe de Proyecto al Encargado de Seguridad de la Información.
- Las acciones concretas del flujo entre entornos pre-productivos hacia Producción son definidas en el procedimiento PRO-SSI-14.1 "SUBTRANS-DGTP Procedimiento Recepción de Software de Terceros".

5.2 Separación de Ambientes de Desarrollo, Prueba y Producción

- Los ambientes a gestionar son:
  - Ambiente de Producción: Es la plataforma tecnológica dispuesta para alojar las aplicaciones que usan los usuarios para realizar sus funciones.
  - Ambiente de Desarrollo: Es donde se instalan los sistemas informáticos para el desarrollo de aplicaciones o sistemas de información. También es la infraestructura para instalar software propietario que debe ser personalizado para posterior uso en la Subsecretaría.
  - Ambiente de Pruebas: o Testing o QA (Quality Assurance). Es un ambiente en que se disponibiliza Sistemas de Información recientemente desarrollado o Personalizado para que sea medido por los usuarios finales desde el punto de vista funcional y por la Unidad de TIC para pruebas de estrés, rendimiento y seguridad. Las pruebas son la última etapa de un software en desarrollo o personalización antes de pasar a la etapa de implementación y posterior puesta en producción.
- Se mantendrán, para los 3 entornos de trabajo: desarrollo, test y producción.
  - Separación de red: segmentos de red, distintos grupos de IP.
  - Separación de la base de datos.
  - Separación de roles. Los roles de seguridad a cargo de los distintos ambientes y sus transiciones:
    - Desarrollo: Solo el equipo del Proyecto.
    - Testing, contará con un Encargado de transferencia a testing
    - Producción: El encargado de Infraestructura de la Unidad de TIC.
- 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.
- Entre otros se debe velar por diferenciar para cada entorno:
  - Separación de equipos y sistemas operativos
  - Los niveles de pruebas asignados y los datos para ellas.
  - Los controles de acceso deben diferenciar cada entorno para su autorización.
  - Se debe configurar perfiles distintos e identificar el entorno accesado.
- El software de desarrollo y productivo se debe ejecutar en distintos ambientes tecnológicos o procesadores de computador, así como también se debe separar las redes en donde están instalados.

- El Área de Infraestructura es responsable de mantener la confidencialidad de las contraseñas con privilegios superiores en los sistemas en producción.
- Por su lado, el Encargado de Seguridad de la Información debe custodiar las credenciales de acceso de todos los Activos de Información de la Subsecretaría.
- Se deben probar los cambios a los sistemas y aplicaciones en un entorno de pruebas o etapas antes de aplicarlos a los sistemas que están en producción.
- A no ser que sea bajo circunstancias excepcionales y que estén aprobadas por el Encargado de la Unidad de TIC, no se deben realizar pruebas en los sistemas que están en producción.
- Los compiladores, editores y otras herramientas de desarrollo no deben estar accesibles desde los sistemas de producción cuando sean innecesarios.
- Los usuarios deberían utilizar distintos perfiles de usuario para los sistemas en producción y de prueba y se deberían mostrar menús para mostrar mensajes de identificación adecuados para reducir el riesgo de errores.
- Los datos sensibles no se deberían copiar en el entorno del sistema de pruebas a menos que se entreguen controles equivalentes para el sistema de pruebas.

5.3 Seguridad del entorno de 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.
- La empresa externa que trabaje con códigos de sistemas críticos debe firmar una carta de confidencialidad.
- Debe existir un repositorio único y controlado de código fuente de la Institución.
- El desarrollo de los sistemas se realiza en un ambiente local, utilizando los datos de la base de datos de desarrollo.
- El desarrollador es responsable de mantener su ambiente local libre de fuentes de virus, troyanos, gusanos y otros que pudieran comprometer su desarrollo.
- El desarrollo se basa en el documento de levantamiento de requerimiento.
- Las pruebas del sistema deben incluir: pruebas de integración (instalación, almacenamiento, configuración, seguridad, recuperación ante errores), pruebas funcionales y de rendimiento. Estos deben quedar registrados.
- El control de acceso usado en el ambiente de testing debe ser tan estricto como el usado en el ambiente de producción.

- El usuario solicitante accede al ambiente de testing y solo tienen acceso a lectura de la información.
- Los sistemas críticos:
  - Deben incluir la validación de los datos de entrada, para asegurar un correcto procesamiento.
  - deben incluir controles de validación de los datos de salida, para asegurar que el procesamiento ejecutado haya sido correcto.
  - que interactúen con otros deben incluir controles para asegurar la integridad de los mensajes intercambiados.

5.4 Paso a producción y seguridad del entorno de Producción.

- El paso a producción del proyecto de desarrollo es autorizado por el usuario solicitante, denominado "Cliente Líder".
- El jefe de Proyecto debe solicitar el paso a producción verificando un conjunto claramente establecido de documentos y condiciones verificadas, lo que debe dejar registros auditables.
- Según el proyecto se define el tiempo 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 ("Pruebas de Desarrollo") antes de pasar a la etapa de pruebas formales en QA o Entorno de Pruebas.
- El equipo QA de pruebas ("Pruebas de QA"), debe revisar y auditar los controles de seguridad, según las especificaciones generadas en la etapa de diseño.
- Si hay modificaciones importantes 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 del usuario final del sistema, debidamente coordinados con el área dueña del sistema.

5.5 Segregación de redes

- Un método para administrar la seguridad de redes de gran tamaño es dividirlas en distintos dominios de red. Los dominios se pueden seleccionar en base a niveles de confianza (es decir, dominio de acceso público, dominio de escritorio, dominio de servidor), junto con unidades organizacionales (es decir, recursos humanos, finanzas, marketing) o alguna combinación (es decir, el dominio del servidor que se conecta a varias unidades organizacionales). La segregación se puede realizar mediante redes con diferencias físicas o mediante el uso de distintas redes lógicas (es decir, conexión de redes privadas virtuales).
- Se debe definir correctamente el perímetro de cada dominio

5.6 Control de Cambios

- La introducción de nuevos sistemas y los principales cambios a los sistemas existentes deben seguir un proceso formal de documentación, especificaciones, pruebas, control de calidad e implementación administrada.
- Para sistemas relevantes, se debe incluir una evaluación de riesgos, análisis de los impactos de los cambios a introducir y la especificación de los controles de seguridad necesarios.

- Se debe cautelar que los controles de Seguridad de la Información existentes no se vean comprometidos.
- Se debe obtener acuerdo formal de aprobación y vuelta atrás de cualquier cambio significativo.

5.7 Instalación del software en sistemas operacionales

- Toda actualización de software en entorno productivo, incluidas aplicaciones, y bibliotecas de programas deben ser realizadas sólo por los Ingenieros de Sistemas del área de Infraestructura y con la debida autorización.
- En el entorno productivo no puede instalarse código ejecutable no aprobado, o código aún en desarrollo. Tampoco debe instalarse compiladores o utilitarios de desarrollo.
- Las aplicaciones y el software productivo deben ser implementados sólo después de haber efectuado las pruebas exigidas y siguiendo los protocolos formalmente diseñados.
- Se debe mantener actualizado y controlar las configuraciones y documentación de todo sistema productivo.

5.8 Principios de ingeniería de sistema seguro

- Se deben identificar y establecer como estándar Institucional los criterios de seguridad mínimos o por nivel de criticidad del sistema que se deben solicitar y verificar en los sistemas de información que se desarrollen para la Institución.
- Dichos criterios deben plasmarse como técnicas de ingeniería para desarrollo seguro, orientadas, por ejemplo, a:
  - Identificación y Autenticación de usuarios.
  - Modelos de Roles y Perfiles de Autorización.
  - Control y validación de datos de sesión seguros.
  - Sanitización y eliminación de códigos de depuración.
- Se deben considerar todos los aspectos de la arquitectura, considerando negocios, datos, aplicaciones, tecnología y entorno, equilibrando la necesidad de la seguridad de la información con las del negocio.
- Se debe analizar nuevas tecnologías y sus riesgos de seguridad, manteniendo test de pruebas de seguridad de la información para patrones de ataque conocidos.

5.9 Gestión de pruebas de Seguridad y Aprobación del sistema

- Tanto las pruebas en Ambiente de Desarrollo como QA, deben considerar los requisitos de seguridad de la información.
- Las pruebas deben quedar registradas en Plan de Pruebas y deben considerar tanto por componentes como por sistema integrado.
- Se debe validar que las pruebas sean robustas y no introducirán vulnerabilidades.
- Los mecanismos de control de acceso, que se aplicarán a los sistemas de información en producción, deben aplicarse también durante las pruebas.
- Para toda prueba debe planificarse también los controles de seguridad a revisar.

6. REGISTROS DE OPERACIÓN Y/O LOGS

Son registros de operación de este Instructivo:

- Mail del Jefe de Proyecto al Encargado de la Unidad de TIC y al Encargado de Seguridad de la Información con reporte de adherencia y cumplimiento del nuevo proyecto a la normativa vigente del SSI-MTT.

7. EXCEPCIONES AL CUMPLIMIENTO DEL PRESENTE INSTRUCTIVO

Frente a casos de especiales, el Jefe de la Unidad de Informática de la Subsecretaría evaluará la situación y podrá establecer condiciones puntuales de excepción en el cumplimiento del presente procedimiento, siempre que no infrinja las políticas internas existentes. Toda excepción debe ser documentada y monitoreada, generando un proceso de revisión del procedimiento, para determinar si se deben efectuar actualizaciones en las condiciones de operación particular.

8. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

El completo glosario de términos y siglas utilizados en los documentos del Sistema de Gestión de Seguridad de la Información de la Subsecretaría de Transporte, se encuentran integrados en el Estándar de Seguridad "Glosario Términos de SSI-MTT", ubicado en la sección Políticas de Seguridad de la Información de la intranet institucional.

9. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
0	11/2017	Creación	Todas	RM
1	12/2017	Creación	Todas	RM