GOBIERNO REGIONAL DE LOS RÍOS

Región de Los Ríos
GOBIERNO REGIONAL

PROCEDIMIENTOS DE DESARROLLO TERCIARIZADO

Sistemas de Gestión de Seguridad de la Información
(SGSI- ISO/IEC 27001-27002)

Control: **A.12.01.04 Separación de los ambientes de desarrollo, prueba y operacionales**

Control: **A.14.02.07 Desarrollo tercerizado**

Control: **A.14.02.08 Prueba de seguridad del sistema**

Control: **A.14.02.09 Prueba de aprobación del sistema**

Control: **A.14.03.01 Protección de datos de prueba**

Contenidos Página

Contenido

I. Versiones

Fecha	Versión	Creador	Modificación o actualización
08-11-2019	1.0	Patricio Acum Salinas	Primera versión

II. Introducción

El Gobierno Regional de Los Ríos, es un organismo autónomo con personalidad jurídica de derecho público, que tiene por objetivo la administración, el desarrollo social, cultural y económico de la región, su principal herramienta de inversión el F.N.D.R. (Fondo Nacional de Desarrollo Regional) y su misión como institución pública es "Liderar de manera integrada el desarrollo de la Región de Los Ríos, acorde a principios de participación, equidad, integración territorial y sustentabilidad, con el fin de mejorar la calidad de vida y bienestar de sus habitantes, mediante la formulación e implementación de instrumentos de planificación, coordinación y gestión de la inversión pública."

Durante el desarrollo de los procesos tendientes al logro de los objetivos y misión institucional, se ve involucrada una gran cantidad de información, de medios y sistemas en los que ésta se procesa y de funcionarios y personas que prestan servicios a la institución y/o externos que se relacionan con la institución en las distintas etapas de los procesos. Todo lo anterior forma parte de los **"Activos de Información del Gobierno Regional de Los Ríos",** dichos activos requieren de un adecuado resguardo ante posibles amenazas o incidentes que afecten a la seguridad de los mismos.

El Gobierno Regional de Los Ríos, en cumplimiento con el Sistema de Gestión de Seguridad de la Información y los controles asociados a la Norma SGSI- ISO/IEC 27001-27002 referentes al desarrollo tercerizado, mediante el presente documento establece el **PROCEDIMIENTOS DE DESARROLLO TERCIARIZADO** que en adelante será la guía para informar a empresas externas y a los funcionarios del Gobierno Regional de la importancia de la seguridad de la información en este sentido

III. Objetivo

Los objetivos generales del presente procedimiento, se enmarcan el sistema de seguridad de la información del Gobierno regional de Los Ríos y son los siguientes:

- 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.

IV. Alcance

El alcance del presente documento involucra a todos los funcionarios del Gobierno Regional, independiente de su calidad jurídica 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.14.02.07	Desarrollo tercerizado
A.14.02.08	Prueba de seguridad del sistema
A.14.02.09	Prueba de aprobación del sistema
A.14.03.01	Protección de datos de prueba

V. Referencias

- ✔ NCh ISO 27002
- ✔ Guía Metodológica 2019 (SGSI)
- ✔ Política de Seguridad de la Información Gobierno Regional de Los Ríos
- ✔ Manual de Procedimientos del Usuario

VI. Roles y responsabilidades

Jefatura de Unidad, Departamento o División:

- Apoyar las acciones de difusión del procedimiento, con asistencia a los eventos planificados por este concepto y procurando la asistencia de los funcionarios bajo su cargo.

Unidad de Informática

- Implementar los diferentes externos de desarrollo
- Disponibilizar ambientes de testing
- Coordinar el correcto uso de este procedimiento

Encargado/a de Seguridad de la información:

- Difundir este procedimiento.
- Coordinar revisiones y actualizaciones en el cumplimiento de este procedimiento.

Funcionarios(as) del Gobierno Regional de Los Ríos:

- Informarse y cumplir a cabalidad el este procedimiento.

VII. Definiciones

a. 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

VIII. Modo de Operación

a. Definiciones de desarrollo externo 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.

b. 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.
- 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.

c. 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.

d. 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.

e. 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.

IX. Registro de Operación

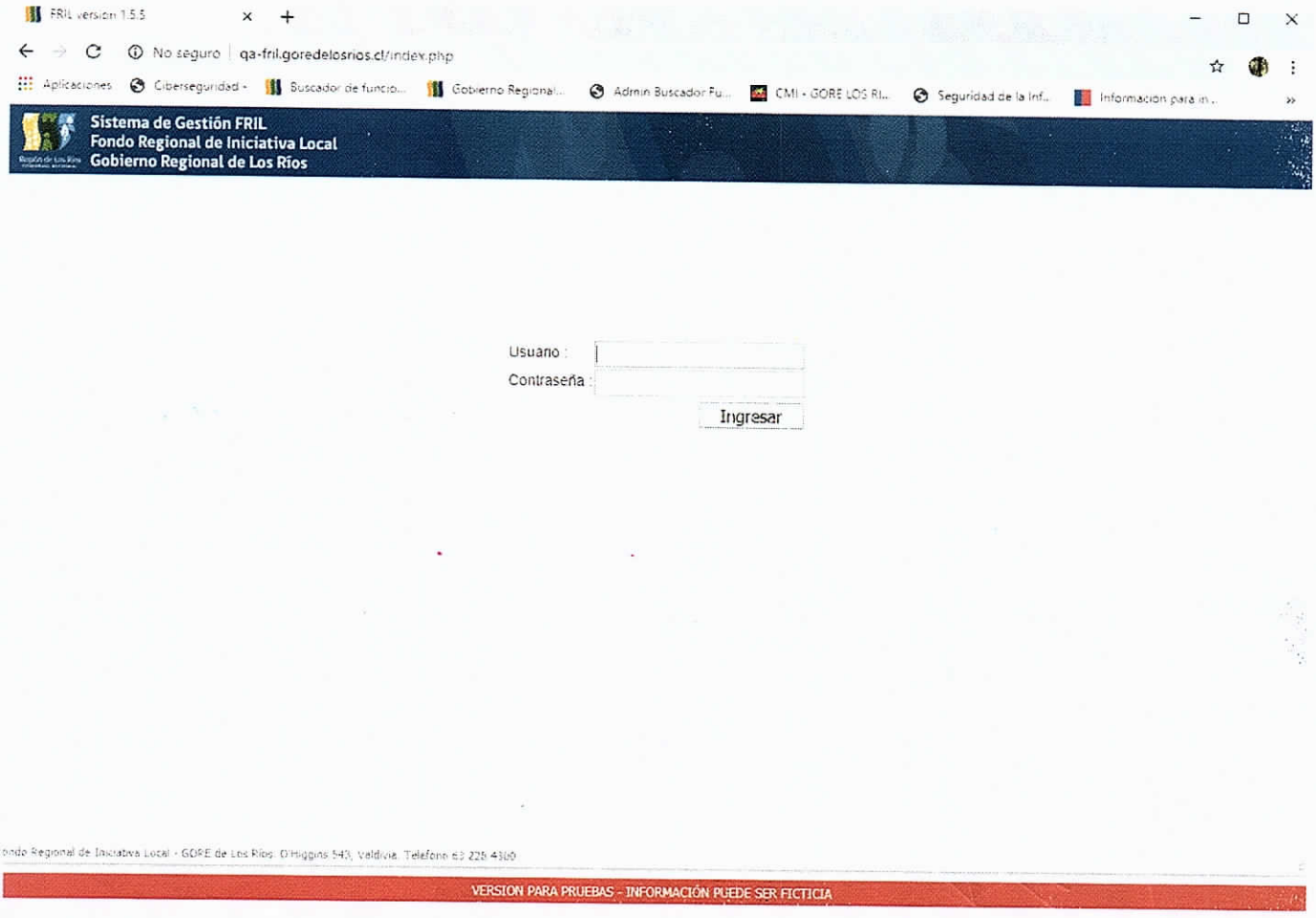
- Print de pantalla de sistemas de testing disponibles en el caso de existir proyectos de desarrollos externalizados, firmado por el Encargado de la Unidad de Informática del Gobierno regional de Los Ríos.
- Acta de validación de paso de testing a producción de los profesionales requirentes del Gobierno Regional de Los Ríos.

X. Validez y Gestión de Documentos

Elaborado por:		
Patricio Acum Salinas	Profesional Unidad de Informática	
Revisado por:		
Alejandro Paredes Zieballe	Miembro Comité - Administrador Regional	
Carlos Ovando Hernández	Miembro Comité - ESI y Jefe Div. Administración y Finanzas.	
Heidi Machmar Hernández.	Miembro Comité - División De Planificación Y Desarrollo Regional	
Rodrigo Aravena Bustamante	Miembro Comité - Coordinador de PMG Institucional.	
Wilson Monzón Riquelme	Miembro Comité - División de Presupuesto e Inversión Regional	
Cesar Pérez S.	Miembro Comité - Encargado Depto. de Finanzas	
Eduardo J. Fagalde A.	Miembro Comité - _Jefe de División de Desarrollo Social y Humano.	
Ernesto Espinoza Navarrete	Miembro Comité - Jefe de División de Fomento e Industria	

CESAR ASENJO JEREZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

Print de pantalla sistema de pruebas software FRIL



GOBIERNO REGIONAL
UNIDAD
INFORMATICA
GORE DE LOS RIOS

Luis Patricio Acum Salinas
Encargado de Unidad de Informática
Gobierno Regional de Los Ríos

Valdivia, Diciembre 2019.