Subsecretaría de Agricultura

POLÍTICA DE DESARROLLO EXTERNALIZADO

Código:	TI-SSI-16
Versión:	2.0
Fecha de la versión:	20-12-2017
Modificado por:	Daniel Coronado Rojo
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
13/08/2015	1.0	Daniel Coronado	Al no existir una política que ampare el desarrollo externalizado, se crea esta política.
20/12/2017	2.0	Daniel Coronado	Se revisa y modifica los campos según la vigencia del contenido, de acuerdo con lo existente en la subsecretaría. Se actualizan los datos referentes a la legislación vigente y los requisitos contractuales. Se agregan los campos de "Ámbito de ejecución, y Alcance" (pág. 4), "control legal y normativo" (pág. 4), y "Documentos de referencia" (pág. 5).

Nota de enfoque 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 el 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 representen siempre a todos/as.

Nota de confidencialidad

Tabla de Contenido

Clasificación del Documento

Nivel de Confidencialidad: Uso Interno.
Nota de Confidencialidad: Documento disponible sólo a funcionarios de la Subsecretaría de Agricultura y personal externo autorizado.

1. Objetivo

Para garantizar que la integridad, la disponibilidad y la confidencialidad de la información que esté presente en todo sistema de información que sea desarrollado por alguna entidad externa, sea preservada, el objetivo del presente documento es establecer unas pautas para el desarrollo externalizado con el fin de:

- Evitar problemas por uso de licencias o códigos fuentes de terceros,
- Evitar problemas de vulnerabilidades por uso de sistemas esenciales, cuyo desarrollo por la entidad externa, no haya cumplido con las medidas de seguridad necesarias, y
- Evitar problemas de funcionamientos de sistema, cuyo uso no sea acorde a las necesidades de la Subsecretaría.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-16 Política de desarrollo externalizado", se aplica a todos quienes cumplen funciones en la Subsecretaría, ya sea en sus instalaciones o fuera de ellas, tanto a funcionarios, así como también, a personas naturales y jurídicas externas, públicas o privadas que presten servicios en la Subsecretaría o para este y que tengan participación en las actividades descritas en este documento.

El ámbito de ejecución de esta política, son todos los activos de información de la Subsecretaría y aquellos bajo su responsabilidad que estén contemplados en el documento. Su cobertura se extiende a la información impresa y también a aquella almacenada electrónicamente, y transmitida por cualquier soporte o medio. Se debe precisar que el presente alcance aplica para los siguientes procesos de provisión de la Subsecretaría de Agricultura: Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.

El Dominio abordado en este documento es el A.14 "Adquisición, desarrollo y mantenimiento de los Sistemas de Información", de la norma NCH ISO 27001:2013.

3. Control legal y normativo

- D.S. N°14/2014. MODIFICA DECRETO Nº 181, DE 2002, QUE APRUEBA REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA, Y DEROGA LOS DECRETOS QUE INDICA,
- D.S. N°83/2004. Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos,
- D.S. N°93/2006. Norma técnica busca minimizar reducción de correos electrónicos masivos en el estado y sus funcionarios,
- D.S. N°1/2015. APRUEBA NORMA TÉCNICA SOBRE SISTEMAS Y SITIOS WEB DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO,
- Ley N°17.336/2004. Ley sobre propiedad intelectual,
- Ley N°19.223/1993. Ley sobre figuras penales relativas a la informática,
- Ley N°19.628/1999. Ley sobre protección de la vida privada,

- Ley N°19.799/2002. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma,
- Ley N°19.927/2004. Ley modifica códigos penales en materia de delitos sobre pornografía infantil,
- Ley N°19.880/2003. Ley sobre procedimientos administrativos que rigen los actos de los órganos del Estado,
- Ley N°20.285/2008. Ley sobre acceso a la información pública,
- Ley N° 19.496. Ley de Protección del Consumidor, N° 19.496, Artículo 28B,
- PNCS. Política Nacional de Ciberseguridad,
- UMyGD. Otras normas Unidad de Modernización y Gobierno Digital y
- Internet Segura – MINEDUC. Internet Segura.

4. Documentos de referencia

- TI-SSI-01 Política General de Seguridad de la Información.
- Norma NCH ISO 27002:2013.
- Cláusulas de seguridad para proveedores.

5. Definiciones

A continuación, una definición de los términos claves utilizados en este documento:

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada

Integridad: Propiedad de la información relativa a su exactitud y completitud.

TI: Tecnologías de la Información.

Licencia de software: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Desarrollo de software: Es la elaboración de un producto de software por medio de metodologías, herramientas existentes o creadas específicamente, y de personas calificadas, con el fin de solucionar una problemática o de cumplir con un requerimiento solicitado.

Código fuente: En el contexto de la informática, el código fuente es el conjunto de líneas de textos de un programa o software (escrita en un lenguaje de programación), cuyo fin es ser las directrices que debe seguir el procesador de la computadora, para realizar y ejecutar dicho programa. Para que el procesador

pueda llevar a cabo esto, se debe utilizar una herramienta llamada compilador (se conocen también como ensambladores, intérpretes, entre otros).

6. Roles y responsabilidades

Para cumplir con los objetivos de la presente política, se establecen los siguientes roles y responsabilidades:

Encargado de Seguridad de la Información: Funcionario a cargo del desarrollo e implementación de la Política del Sistema de Seguridad para el Servicio, así como también, de velar por la correcta aplicación tanto de esta política, como a su vez, de los instrumentos de apoyo utilizado para ello (Políticas y Procedimientos).

Comité de Seguridad de la Información: Es responsable por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades de la Subsecretaría, los recursos disponibles y la normativa vigente.

Jefe Departamento TI: Responsable de definir los dominios de seguridad, implementar medidas de control para las excepciones de acceso directo desde dominios externos hacia servicios de producción entre otros accesos perimetrales de la red, gestionar y controlar el sistema de gestión de seguridad sobre la protección de los activos de información del servicio, conforme a la normativa vigente y los objetivos estratégicos institucionales.

Funcionario Subsecretaría de Agricultura: Responsables de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada, a través de canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

7. Definición respecto a las materias específicas abordadas:

El control del dominio abordado de la norma NCH ISO 27001:2013 en este documento, es el siguiente:

N° Control	Nombre control NCH ISO 27001	Descripción del control
A.14.2.7	Desarrollo tercerizado	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas externalizados.

A continuación, el desglose de las directrices referente a este control:

7.1. Política de desarrollo externalizado (control de referencia A.14.2.7)

En la subsecretaría no existe un departamento dedicado al desarrollo de Softwares y Sistemas, por lo cual cuando se da la necesidad de disponer de un sistema u software para un proceso crítico, se licita el desarrollo a una empresa externa, que tendrá toda la responsabilidad del desarrollo e implementación de software y/o sistema. Al momento de solicitar el desarrollo de un sistema y/o software, se tiene que tomar en cuenta lo siguiente.

7.1.1. Disposiciones legales del código y de la licencia del software y/o sistema

Es necesario revisar que la empresa desarrolladora, disponga de buenos antecedentes y cumpla con las disposiciones legales en cuanto a derecho de autor y/o autoría del sistema u software desarrollado, para evitar posibles problemas legales en cuanto a licencias o derecho de uso.

7.1.2. Requisitos contractuales

La empresa desarrollada debe de disponer de un entorno de desarrollo seguro en todas las etapas del proyecto, desde las etapas de diseño, hasta el resguardo de repositorios, gestión de vulnerabilidades y pruebas del sistema desarrollado.

La empresa desarrolladora deberá cumplir con todos los acuerdos de seguridad de la Subsecretaría.

7.1.3. Pruebas de aceptación de calidad.

El sistema o el software desarrollado, debe ser probado en entornos lo más cercano a la realidad, para determinar su funcionamiento. De ser satisfactorio las evaluaciones, deberá ser expresado a la empresa desarrolladora por escrito, para ser documentado.

7.1.4. Provisión de evidencias

La Empresa desarrolladora, debe demostrar que durante el desarrollo:

- Resguardaron datos sensibles o privados del servicio que hayan utilizados en el desarrollo de la software u sistema.
- El sistema u el software desarrollado, fue probado lo suficiente para determinar vulnerabilidades o formas de prevenir posibles contenidos maliciosos o modificaciones no autorizadas al código fuente.

Para esto, se deberá de provisionar evidencia que se estime necesaria (log de registro, videos...).

7.1.5. Disposiciones de garantía

La empresa desarrolladora debe asegurar que el código fuente del sistema u software desarrollado, no estará disponible para terceros, para así resguardar la integridad del sistema u software que será utilizado por el servicio.

7.1.6. Derecho contractual

Dentro de los acuerdos establecidos con la empresa externa de desarrollo, la subsecretaría debería al menos una vez, realizar una auditoría del proceso y control de desarrollo del sistema u software encomendado, para verificar como se ha ido realizando el proyecto y así tener una mejor noción del estado del servicio solicitado.

7.1.7. Documentación sobre el entorno de desarrollo

La empresa desarrolladora debería facilitar o entregar documentación referente a las herramientas utilizadas en el desarrollo del sistema u software solicitado, vale decir, que tipo de plataforma se usó en el desarrollo del sistema u software, tipo de base de datos utilizado, sistema operativo que trabajará, entre otros.

8. Periodicidad de evaluación y revisión de la política

El propietario de este documento es el Jefe Departamento TI, quien deberá verificar la vigencia del contenido, por lo menos una vez al año. Si el documento necesita ser modificado y/o debe realizarse alguna actualización, tendrá que ser notificado al resto de los miembros del Comité de Seguridad de la Información.

La periodicidad de evaluación del documento debe hacerse al menos una vez al año.

9. Difusión

El "TI-SSI-16 Política de desarrollo externalizado" deberá ser difundida -según lo expresado en la Política General de Seguridad de la Información- por medio de la intranet institucional, o por vía circular o por decreto, y/o vía correo electrónico según sea pertinente, asegurándose una completa cobertura.

10. Validez y gestión de documentos

Este documento es válido desde el 20-12-2017

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes que surgen por fallas en el uso de la plataforma o software licitado
- Cantidad de registros no documentados durante el proyecto de desarrollo licitado
- Cantidad de evidencias que no fueron facilitadas o cuya veracidad sea dudosa.

Creado por:

Ingeniero Proyectos TI
Daniel Coronado Rojo

Validado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DEPTO TECNOLOGIAS DE LA INFORMACION

Jefe Departamento TI
Rafael Reyes Cuevas

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISIÓN ADMINISTRATIVA

Encargado de Seguridad de la Información
Jefe División Administrativa
Jorge Vega Saavedra