Subsecretaría de Agricultura

POLÍTICA DE LA CONTINUIDAD DEL NEGOCIO

Código	TI-SSI-22
Versión:	1.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
20-12-2017	1.0	Daniel Coronado	Para cumplir con el cumplimiento del control A.17.1.1 de la norma NCH ISO 27001:2013, se crea esta política.

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

La información contenida en este documento es de propiedad de la Subsecretaría de Agricultura y debe ser tratada de acuerdo a su nivel de confidencialidad, establecida en la "TI-SSI-07 Política para manejo de información clasificada". El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente a la Subsecretaría de Agricultura

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

Definir el objetivo, el alcance y las reglas básicas necesarias para la gestión de la continuidad del servicio de la Subsecretaría de Agricultura, frente a incidentes o situación perjudicial que altere la normal operatividad de los procesos de provisión.

2. Ámbito de ejecución, y alcance

Esta Política se aplica a todo el Sistema de Gestión de la Continuidad del Negocio (SGCN), que cubre los siguientes procesos de provisión de productos estratégicos 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.17 "Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio", de la norma NCH ISO 27001:2013.

Los usuarios de este documento son todos los funcionarios de la Subsecretaría de Agricultura, que son parte de los procesos de provisión descritos en el párrafo anterior, como también los proveedores que cumplen alguna función en el SGCN.

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.
- Instrumento SSI 2017.
- TI-SSI-18 Plan de continuidad de los servicios.

5. Definiciones

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

Activo: Información o bienes que tiene valor para la organización. Una organización incluye diferentes tipos de activos: activos relacionados con el entorno (edificios, instalaciones, equipamiento) y personal, activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones), activos relacionados con la información (datos, soporte), activos relacionados con las funcionalidades de la organización (productos, servicios) y activos intangibles (credibilidad, conocimiento acumulado).

Activo de Información: Corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. Se distinguen 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.) Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- Los Equipos/Sistemas/infraestructura que soportan esta información
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Activo primario: El activo de información asociado a las funciones sustantivas de una Institución, dentro de los cuales se encuentran la información y los procesos.

Activos de proceso: Los elementos de información que son parte de un proceso y que reflejan características específicas del mismo, entre los cuales se encuentran los procesos de provisión.

Activo de soporte: El que apoya o complementa a un activo primario en su función. En estos se encuentran el hardware, software, redes, personal, sitios, servicios.

Activo de información clave: El activo de información que resulta esencial o estratégico para la operación y/o el control de una infraestructura crítica, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.

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.

Incidente de seguridad: Situación adversa que pone en riesgo un proceso.

Procesos Críticos: Proceso que afecta de forma directa a la satisfacción del cliente y a la eficiencia económica de la organización.

Negocio: Función o servicio prestado por la organización.

Proceso crítico del negocio: Proceso que afecta de forma directa a la satisfacción del cliente y a la eficiencia económica de la organización.

Política de seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de actividades o procesos de interés para la organización.

Propietario de la información: Es el que genera, mantiene y utiliza la información, siendo responsable de ella, y de los procesos que la manipulan, sean éstos manuales, mecánicos o electrónicos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Seguridad de la Información: Conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Sistema de gestión de continuidad del negocio (SGCN): Conjunto de normas o buenas prácticas que ayuda a las organizaciones a establecer estructuras para identificar posibles amenazas, el impacto de los incidentes y cómo pueden protegerse frente a estas. A continuación, el SGCN proporciona a la organización un marco para la gestión mediante estrategias y métodos para reducir el impacto de cualquier incidente, y la creación de la capacidad de respuesta efectiva.

6. Roles y responsabilidades

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

Jefe del Servicio: Responsable de aprobar: la política de seguridad de la información, el encargado de seguridad de la información y el comité de la seguridad de la información. Se encarga además de formalizar la aprobación o la cancelación de los contratos que se tengan con los proveedores.

Encargado de Seguridad de la Información: Funcionario designado por el Jefe de Servicio, con el fin de tener a su cargo el desarrollo e implementación de la Política del Sistema de Seguridad para el Servicio, así

como también, 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: Son responsables 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 de la Subsecretaría de Agricultura: Responsable 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.17.1.1	Planificación de la continuidad de la Seguridad de la Información	La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

A continuación, el desglose de las directrices referente a esta política (control de referencia A.17.1.1):

7.1. Objetivo de la gestión de la continuidad del negocio

El objetivo de la gestión de la continuidad del negocio es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían tener sobre las operaciones de negocios; también sirven para proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

7.2. Relación con los objetivos generales y otros documentos

Con la implementación de la continuidad del negocio, la Subsecretaría de Agricultura, desea cumplir con sus objetivos estratégicos.

La gestión de la continuidad del negocio se implementa conforme a los requisitos enumerados en la lista de requisitos legales, normativos, contractuales y dentro del marco referencial definidos por los siguientes documentos

7.3. Definición de objetivos de continuidad del negocio

El Encargado de Seguridad de la Información es el responsable de definir los objetivos para todo el SGCN y el método para medir el cumplimento de los mismo. El Encargado de Seguridad de la Información o quién designe este tiene la responsabilidad de revisar esos objetivos al menos una vez por año.

Los objetivos para elementos individuales del SGCN son propuestos y documentados por Jefe Departamento TI o quien lo subrogue y autorizados por el Encargado de Seguridad de la Información, estos objetivos deben ser revisados al menos una vez por año por las mismas personas que lo propusieron.

Las acciones para cumplir con estos objetivos serán determinadas en el Plan de tratamiento de riesgos, en el plan de preparación para la continuidad del negocio, con las acciones correctivas y preventivas según el Procedimiento para acciones correctivas y preventivas y en la Revisión por parte de la dirección.

7.4. Alcance

El sistema de gestión de la continuidad del negocio se implementa para toda la Subsecretaría de Agricultura, con especial atención sobre las actividades identificadas durante el análisis de impactos de negocio.

Las ubicaciones de negocio de la organización incluidas en el alcance:

- Edificio Central.
- Oficinas regionales (Seremias), ubicadas en cada capital regional del país.

Unidades organizativas incluidas en el alcance:

- Gestión de Personas (GGPP)
- Departamento de Transferencias
- Área administrativa de cada Seremia regional
- Departamento de Informática (TI).

7.5. Procesos de provisión clave

Los siguientes procesos de provisión clave son identificadas por la Subsecretaría de Agricultura dentro del alcance definido en la sección anterior

- Informe de Factibilidad para la Construcción (IFC).
- Red Agroclimática Nacional (RAN).
- Transferencias de fondos de la Subsecretaría.

La gestión de la continuidad del negocio debe garantizar que los procesos mencionados precedentemente se recuperarán a un nivel predefinido.

Todas las actividades relacionadas con los procesos de provisión, están detalladas en el Plan de continuidad de los servicios.

7.6. Responsabilidades para la gestión de la continuidad del negocio

Responsabilidades generales:

- El Encargado de Seguridad de la Información es el responsable que la gestión de la continuidad del negocio sea establecida e implementada de acuerdo con esta política de proporcionar los recursos necesarios.
- El Jefe Departamento de TI o quién designe este es responsable de la implementación operativa y del mantenimiento del sistema de gestión de la continuidad del negocio.
- El Comité de Seguridad de la Información debe revisar el SGCN al menos una vez por año o cada vez que se produzca una modificación significativa y debe elaborar un informe de la revisión

Responsabilidades específicas

- El Encargado de Seguridad de la Información es el responsable de adoptar e implementar el Plan de capacitación y concientización que corresponda a todas las personas que cumplen una función en la gestión de la continuidad del negocio.
- Los preparativos relacionados con la continuidad del negocio deben ser probados y verificados al menos una vez por año utilizando diversos métodos para evaluar su pueden proteger a las actividades de la organización. Para ellos el Jefe del Departamento de TI o quién designe este debe redactar un Plan de prueba y verificación que debe ser aprobado por el Comité de Seguridad de la Información. Luego de cada prueba y verificación, el Jefe del Departamento de TI o quién designe este debe elaborar un informe de prueba y verificación.
- El Jefe Departamento TI es el responsable de adoptar e implementar el Plan de mantenimiento y revisión del SGCN para que todos los elementos del SGCN estén operativos y actualizados.
- Cada vez que se activa un Plan de continuidad del negocio, un Plan de recuperación o un Plan de respuesta a los incidentes, el Encargado de Seguridad de la Información es responsable de supervisar la influencia de la gestión de la continuidad del negocio.
- El Encargado de Seguridad de la Información es el responsable de supervisar las no conformidades, falsas alarmas, incidentes reales, etc. y de evaluar las acciones preventivas necesarias.

7.7. Medición

La Subsecretaría de Agricultura medirá lo siguiente:

- Si los objetivos definidos de acuerdo a esta Política son cumplidos al menos una vez por año, generalmente antes de la Revisión por parte de la dirección.
- Efectividad y adecuación de los planes de continuidad del negocio según las frecuencias definidas en el mismo Plan de continuidad del negocio

El Encargado de Seguridad de la Información elaborará un informe con los resultados de la medición, mientras que el análisis y evaluación de los resultados se realizará en la revisión por parte de la Comité de Seguridad de la Información.

7.8. Apoyo para la implementación del SGCN

A través del presente, el Jefe del Servicio declara que en todos los elementos de la implementación del SGCN se contará con el apoyo de los recursos adecuados para lograr todas las metas y objetivos establecidos en esta Política como también para cumplir con todos los requisitos identificados.

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-22 Política de la continuidad del negocio" 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 para los funcionarios, como también los proveedores que cumplen una función en el SGCN.

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 funcionarios y proveedores que no aparecen en este documento
- No-conformidad de gestión de la continuidad del negocio con disposiciones legales, obligaciones contractuales y demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGCN.
- Responsabilidades asignadas para la implementación del SGCN.

Creado por:

Ingeniero Proyectos TI
Daniel Coronado Rojo

Validado por:

SUBSECRETARÍA DE AGRICULTURA
JEFE DEPTO TECNOLOGIAS DE LA INFORMACION

Jefe Departamento TI
Rafael Reyes Cuevas

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISION

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