Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACION PARA EL SERVIU REGION DE AYSÉN DEL GENERAL CARLOS IBÁÑEZ DEL CAMPO Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 2496 DEL 2012 SERVIU REGION DE AYSEN EN SU VERSIÓN 1.2.

RESOLUCION EXENTA N° 1181

COYHAIQUE, 05 AGO. 2013

VISTOS:

a. Lo dispuesto en el D.L. N° 1.305, de 1975 que Reestructura y Regionaliza el Ministerio de Vivienda y Urbanismo;

b. Lo dispuesto en el D.S. N° 83 del 2004 (MINSEGPRES), que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos;

c. Lo dispuesto en la Norma Chilena Nch – ISO 27002.Of2009 (INN), sobre Tecnología de la información – Código de prácticas para la gestión de seguridad de la información.

d. La Resolución Exenta N° 2496 del 2012 Serviu Región de Aysén del General Carlos Ibañez del Campo, que aprueba la Política de Seguridad de la Información para este Servicio en su versión 1.2.;

e. La Resolución Exenta N° 1839 del 2012 Serviu Región de Aysén del General Carlos Ibañez del Campo, que designa y fija funciones a la encargada y al comité de seguridad de la información de esta institución.

f. La Resolución N° 1.600, del 2008 de la Contraloría General de la República que fija las normas sobre exención del trámite de toma de razón;

g. Las facultades que me confieren el D.S. 355 de 1976. de (V. y U),y el Decreto N° 74 fecha 29/12/2011, ambos del MINVU, que me designa como Director Serviu Región de Aysén; y

CONSIDERANDO:

a. Que el Comité de Ministros de Desarrollo Digital y la Secretaria de Desarrollo Digital, comprende la incorporación de Tecnologías de Información en las Comunicaciones de los Órganos de la Administración del Estado, con el fin modernización del estado mediante el desarrollo de e-gobierno.

b. Que se han dictado una serie de normas técnicas entre las que se encuentra el Decreto Supremo N° 83 del 2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Organismos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos y la Norma ISO

27001.Of2009 que proporciona un marco de gestión de la seguridad de la Información utilizable por cualquier tipo de organización, pública o privada.

c. Que la actual política de seguridad de la información, aprobada por Resolución Exenta N° 2541 del 2011 Serviu Región de Aysén del General Carlos Ibáñez del Campo, no contempla aspectos relevantes, por lo que se hace necesaria su actualización.

d. Que, de conformidad con lo previsto en el articulo 11 del Decreto Supremo N ° 83 citado, es necesario actualizar la Política de seguridad de la Información contemplada en la Resolución Exenta N° 2541 del 2011 Serviu Región de Aysén del General Carlos Ibáñez del Campo; y en el control A 5.1.1. de la Norma ISO 27001.Of2009, en conformidad a lo señalado precedentemente, dicto lo siguiente:

RESOLUCIÓN:

1. Apruébase la Política de Seguridad de la Información para el SERVIU Región de Aysén del General Carlos Ibañez del Campo en su versión 1.2., cuyo texto se entiende forma parte íntegra de la presente Resolución.

2. Establécese que es obligación de la Encargada de Seguridad de la Información del Serviu Región de Aysén de efectuar la difusión de la política fijada por este instrumento, así como también realizar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.
3. Déjese sin efecto, a partir de la total tramitación del presente acto administrativo, aquella política aprobada a través de la Resolución Exenta N° 2541 del 2011 Serviu Región de Aysén del General Carlos Ibañez del Campo.
4. Se deja constancia que la presente Resolución no irroga gastos para el presupuesto de este Servicio.

ANÓTESE, NOTIFÍQUESE, CÚMPLASE Y ARCHÍVESE.

NELSON QUINTEROS FUENTES
INGENIERO CIVIL
DIRECTOR SERVIU REGION DE AYSEN

PRF/IIM/VMM/ENC/MVR/GSM/RRB/GCR/CNZ
DISTRIBUCION A :
- Jefes Departamentos (5)
- Delegación Provincial Aysén
- Encargado PMG
- OIRS
- Encargado Sección Personal
- Contralor Regional
- Oficina de partes.

POLÍTICA DE SEGURIDAD DE LA INFORMACION SERVIU REGIÓN DE AYSEN DEL GENERAL CARLOS IBÁÑEZ DEL CAMPO

REVISIONES DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN				
N° Rev.	Fecha Aprobación	Motivo de la revisión	Pags. Modif.	Autor(es)
1.0		Elaboración Inicial	Todas	Claudia Novoa Zamora
1.1.	Dic. 2011	Correcciones de contenido	Todas	Claudia Novoa Zamora
1.2.	Oct. 2012	Correcciones de contenido	Todas	Claudia Novoa Zamora
1.3.	Agosto 2013	Correcciones de contenido	9	Claudia Novoa Zamora

1. MARCO GENERAL

La información es un activo esencial para que el Serviu Región de Aysén del General Carlos Ibáñez del Campo pueda alcanzar los objetivos estratégicos que se ha trazado y así cumplir con la misión que le ha sido encomendada. Se entiende por activo de información a todos aquellos elementos que hacen posible o sustentan los procesos de negocio u operativos, que pueden ser las personas que utilizan la información y que tienen conocimientos de los procesos institucionales; equipos, sistemas e infraestructura que soporta la información y; la información propiamente tal en cualquiera de sus múltiples formatos, tales como papel, digital, texto, imagen, audio, video, entre otros.
Estos activos, se exponen a potenciales vulnerabilidades y amenazas que podrían comprometer la continuidad operacional de la Organización tales como: el riesgo de robo, divulgación o mal uso, pérdida por eliminación accidental, y cualquier otro. La gestión de seguridad de la información busca proteger todos los activos de información con el fin de asegurar su **Confidencialidad, Integridad y Disponibilidad** y para ello es fundamental definir e implementar una estrategia que incluya un modelo de políticas y controles específicos que sean revisados periódicamente, generando así una mejora continua de la seguridad de los activos de información, en coherencia con los distintos procesos institucionales.

2. DECLARACIÓN INSTITUCIONAL

El Serviu Región de Aysén del General Carlos Ibáñez del Campo promueve y apoya el cumplimiento del DS N° 83 del 2004 (MINSEGPRES), lo que implica un compromiso para proteger los activos de la información institucional de amenazas, riesgos, etc.; así como también, de desarrollar y ejecutar un plan de acción de mejora continua de modo de asegurar una adecuada gestión de seguridad de la información en sus diferentes ámbitos de aplicación.

3. TERMINOS Y DEFINICIONES

3.1. SEGURIDAD DE LA INFORMACIÓN

3.1.1. **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

3.1.2. **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

3.1.3. **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

3.1.4. Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya se magnético, en papel, en pantallas de computadoras, audiovisual u otro.

3.1.5. Sistemas de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

3.1.6. Tecnologías de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

3.1.7. Activos de la Información: Corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución.

3.1.8. 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 Servicio.

3.1.9. **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 la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

3.1.10. **Comité de Seguridad de la Información:** El comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Servicio, destinado a garantizar el apoyo manifiesto de la autoridad a las iniciativas de seguridad.

3.1.11. **Responsable de la Seguridad Informática:** Es la persona que cumple la función de supervisar el cumplimiento de la presente política y asesorar en materia de seguridad de la información a los integrantes del Servicio que así lo requieran.

3.1.12. **Incidentes de Seguridad:** Un incidente de seguridad es un evento adverso en un activo de la información, que compromete la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad, un intento o amenaza de romper los mecanismos de seguridad existentes.

4. DEFINICIÓN DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

La seguridad de la información se entiende como la preservación de las características de **Confidencialidad, Integridad, Disponibilidad.**

Adicionalmente, deberán considerarse los conceptos de:

a. **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información validando al emisor para evitar suplantación de identidades.

b. **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

c. **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

d. **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

e. **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

f. **Confiabilidad de la Información**: es decir que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

5. OBJETIVOS DE LA GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información en el Serviu Región de Aysén del General Carlos Ibáñez del Campo, tiene como principales objetivos:

- Proteger los activos de información Institucional.
- Implementar y propender al cumplimiento de las políticas generales y específicas, normas, procedimientos, prácticas y estándares referentes a la seguridad de la información.

- Clasificar correctamente la información e implementar mecanismos de seguridad adecuados a sus características.

- Realizar una evaluación de riesgos periódica, cuyos resultados ayudarán a orientar la implementación de controles para proteger la información afecta a dichos riesgos.

- Implementar técnicas para la gestión del riesgo utilizando como base la NCh-ISO 27005.0f2009.

- Impulsar el desarrollo, cumplimiento y mantenimiento de un Plan de Continuidad de Negocio el que debe entenderse como un proceso de carácter cíclico y continuo.

- Realizar difusión permanente de las Directrices de Seguridad de la información, con el objeto de culturizar a todos los usuarios del Serviu Región de Aysén del General Carlos Ibáñez del Campo, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores del Servicio en el cumplimiento de las medidas de seguridad establecidas.

- Revisar, monitorear, auditar y mejorar continuamente las directrices de seguridad que garanticen el mantenimiento de los niveles de seguridad requeridos.

- Destinar los recursos necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre costo y beneficio.

- Cumplir la normativa atingente.

6. ALCANCE

Esta Política de Seguridad de la información se aplica en todo el ámbito del Servicio, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.
Es decir, esta política define las directrices de la Seguridad de la Información para todas las unidades de trabajo, Secciones, Departamentos, Delegación Provincial y prestadores de servicio externos en el SERVIU Región de Aysén del General Carlos Ibáñez del Campo, que permitan preservar la confidencialidad, integridad y disponibilidad de la información. Los ámbitos de acción relacionados con el contenido de la política son el uso de Internet y correo electrónico, uso de software autorizado en la plataforma tecnológica de la Institución, uso de servicios de mensajería, uso adecuado de los recursos informáticos, obligaciones y responsabilidades de los usuarios/as.

7. AMBITO DE APLICACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El ámbito de aplicación de la Política de Seguridad contempla los dominios contenidos en la Nch-ISO 27002.2009 y que son los siguientes:

Ámbito de Control	Referencia Norma NCh-ISO 27002.Of2009	Referencia DS N° 83 de 2005 (SEGPRES)
Política de seguridad	A.5	Art. 11
Organización de seguridad de la información	A.6	Art. 12
Gestión de Activos	A.7	Arts. 13 al 16
Seguridad asociada a los recursos humanos	A.8	Arts. 20 y 21
Seguridad física y del ambiente	A.9	Arts. 17 al 19
Gestión de las comunicaciones y operaciones	A.10	Arts. 22 al 26
Control de acceso	A.11	Arts. 27 al 33
Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12	Art. 34
Gestión de incidentes de seguridad de la información	A.13	No Hay.
Gestión de continuidad del negocio	A.14	Art. 35
Cumplimiento	A.15	No Hay.

1. Política de seguridad: Proporciona a la Institución la dirección y soporte para la seguridad de la información en concordancia con los requerimientos institucionales y las leyes y regulaciones pertinentes.
2. Organización de la seguridad de la información: Orientado a administrar la seguridad de la información dentro del Servicio y establecer un marco gerencial para controlar su implementación.
3. Gestión de Activos: Destinado a mantener una adecuada protección de los activos del Servicio.
4. Seguridad asociada a los recursos humanos: Orientado a reducir los riesgos de error humano, omisión de ilícitos en el Servicio o uso inadecuado de las instalaciones.
5. Seguridad física y del ambiente: Destinado a impedir accesos no autorizados, daños e interferencia a las unidades, departamentos e información del Servicio.
6. Gestión de las comunicaciones y operaciones: Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
7. Control de acceso: Orientado a controlar al acceso lógico a la información.
8. Adquisición, desarrollo y mantenimiento de los sistemas de información: Orientado a garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software.
9. Gestión de incidentes de la seguridad de la información: Destinado a asegurar que las debilidades y eventos de seguridad de la información asociados a sistemas de información son comunicados de manera que permita tomar acciones correctivas a tiempo.
10. Gestión de continuidad del negocio: Dirigido a considerar los aspectos de seguridad de la información y la gestión de continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.
11. Cumplimiento: Orientado a evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual legal y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los sistemas de información.

8. ROLES Y RESPONSABILIDADES

Para llevar a cabo y precaver el cumplimiento de lo indicado en estas políticas, se han definido roles y responsabilidades, los que se desarrollaran en forma paulatina conforme a la madurez del sistema de gestión de seguridad de la información del Serviu Región de Aysén del General Carlos Ibáñez del Campo.

8.1. Comité de Gestión de Seguridad y Confidencialidad de la Información del Serviu Región de Aysén del General Carlos Ibáñez del Campo.

Procederá a revisar y aprobar la Política de Seguridad de la Información y las instrucciones generales de Gestión de Seguridad de la Información, monitorear los cambios significativos en la exposición de los bienes de información a amenazas mayores; revisar y monitorear los incidentes de seguridad de la información que afecten la Gestión del Serviu Región de Aysén del General Carlos Ibáñez del Campo, a fin de establecer acciones preventivas y correctivas; aprobar iniciativas para mejorar la seguridad de la información crítica para la gestión de este Servicio.

El Comité estará compuesto por funcionarios/as del Serviu Región de Aysén del General Carlos Ibáñez del Campo, que sean representantes estratégicos en las distintas áreas del servicio, por lo que a lo menos estará compuesto por:

- Jefes de Departamento (Técnico, Jurídico, Programación y Control, Operaciones Habitacionales)
- Delegado/a Provincial de Puerto Aysén
- Encargado Sección Personal
- Encargado del Programa de Mejoramiento de la Gestión.
- Encargado/a Oficina de Informaciones, Reclamos y Sugerencias.
- Encargado/a de Seguridad de la Información Serviu Región de Aysén del General Carlos Ibáñez del Campo.

8.2. Encargado/a de Seguridad de la Información Serviu Región de Aysén del General Carlos Ibáñez del Campo.

Tiene las siguientes responsabilidades:

a. Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior del Serviu Región de Aysén del General Carlos Ibañez del Campo, el control de su implementación, y velar por su correcta aplicación;
b. Coordinar la respuesta a incidentes que afecten a los activos de información institucional;
c. Establecer puntos de enlace con Encargados de Seguridad de otros Organismos Públicos y especialistas externos que le permita estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

9. POLÍTICAS DE SEGURIDAD ESPECÍFICAS

Para dar lineamientos y estándares de cumplimiento con el propósito de regular aspectos específicos relacionados con la Seguridad de la Información y que tengan directa relación con los ámbitos de control específicos o dominios indicados en la norma NCh27002. Of2009, se dictarán políticas de seguridad específicas.

10. GESTACION DE UNA POLITICA

El desarrollo de nuevas políticas específicas estará enfocado inicialmente en cubrir las brechas para el cumplimiento de los controles específicos incluidos en los distintos ámbitos de control o dominios contemplados en la norma NCh-27002.0f2009.
Las modificaciones a políticas vigentes deberán ser gestionadas a través del Encargado de Seguridad de la Información del Serviu Región de Aysén del General Carlos Ibáñez del Campo, quién a su vez deberá evaluar en conjunto con las partes involucradas la factibilidad de aplicarlas.

11. APROBACION DE UNA POLÍTICA

Las nuevas políticas serán propuestas al Comité de Gestión de la Información por el Encargado de Seguridad de la Información del Serviu Región de Aysén del General Carlos Ibáañez del Campo, quién solicitará su aprobación, informando al Comité sobre su criticidad e importancia de implementación y destacando los riesgos bajo los cuales se encuentran los activos de información que se requieren proteger.

12. DIFUSIÓN DE LA POLITICA

El objetivo principal de la difusión es comunicar la importancia de proteger la información fomentando una cultura de seguridad. El Serviu Región de Aysén del General Carlos Ibáñez del Campo deberá comunicar esta política a todos funcionarios/as de planta, contrata, trabajadores a honorarios, asesores, consultores, practicantes, y otros trabajadores.
La difusión deberá efectuarse de manera que el contenido de la política sea accesible y comprensible para los usuarios, para lo que podrá utilizar todos los canales de difusión con los que el Serviu Región de Aysén, del cual tenga disponible, es decir, pagina Web Http://xi.serviu.cl, correo electrónico, entre otros.

13. REVISIÓN Y EVALUACIÓN PERIODICA

La Política de Seguridad de la Información deberá ser redactada por la Encargada de Seguridad de la Información, quién en conjunto con el Comité de Seguridad de la Información serán los responsables de mantenerla y revisarla. Los cambios en la política serán el reflejo de cambios que puedan producirse, tales como: enfoques a la gestión de seguridad, circunstancias del negocio, cambios legales, cambios del ambiente técnico, recomendaciones realizadas por la autoridad pertinente, tendencias relacionadas con amenazas y las vulnerabilidades, entre otras.
Reevaluándose en forma periódica, a lo menos cada 3 años, al igual que la periodicidad con que se evaluará su cumplimiento

14. POLÍTICAS SEGURIDAD DEFINIDAS POR EL MINVU APLICABLES EN EL SERVIU REGION DE AYSÉN

14.1. La Resolución Exenta N° 6710 del Ministerio de Vivienda y Urbanismo establece Política de uso de SIMI (servicio institucional de mensajería instantánea).

14.2. La Resolución Exenta N° 9612 de fecha 27 de Diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba política específica de uso de servicio de mensajería instantánea.

14.3. La Resolución Exenta N° 9613 de fecha 27 de diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba la política específica de navegación en internet.

14.4. La Resolución Exenta N° 9614 de fecha 27 de diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba la política específica de uso de Software.

14.5. La Resolución Exenta N° 9615 de fecha 27 de diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba la política específica de uso de contraseñas.

14.6. La Resolución Exenta N° 9617 de fecha 27 de diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba la política específica de correo electrónico.

14.7. La Resolución Exenta N° 9618 de fecha 27 de diciembre del 2011, del Ministerio de Vivienda y Urbanismo que aprueba la política específica de uso de red informática.

15. NORMATIVA ATINGENTE

La normativa atingente al sistema de seguridad de la información contempla:

1) Ley N° 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.
2) Ley N° 19.628, sobre protección de la vida privada y datos personales.
3) Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado.
4) Ley N° 17.336, sobre propiedad intelectual.
5) Ley N° 19.223, sobre delitos informáticos.
6) Ley N° 19.927, sobre delitos de pornografía infantil "
7) Ley N° 20.285, que regula el principia de transparencia de la función publica y el derecho de acceso a la información de los órganos de la administración del Estado.
8) Ley N° 19.553, que concede asignación de modernización y otros beneficios que indica.
9) Ley N° 20.212, que modifica las leyes: N°19.553, N°19.882, y otros cuerpos legales, con el objeto de incentivar el desempeño de los funcionarios públicos.
10) Norma Chilena NCh-180 27002.0f2009 sobre Tecnología de la Información - Código de prácticas para la gestión de seguridad de la información.
11) D.S. N° 181 del 2002, del Ministerio de Economía, Fomento y Reconstrucción, que aprueba el reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
12) D.S. N° 77 del 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos y los ciudadanos.
13) D.S. N° 81 del 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos.
14) D.S. N° 83 del 2005, del Ministerio Secretaria General de la Presidencia que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
15) D.S. N° 93 del 2006, del Ministerio Secretaria General de la Presidencia, que aprueba norma , técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los Órganos de la Administración del Estado y de sus funcionarios.
16) D.S. N° 100 del 2006, del Ministerio Secretaria General de la Presidencia que aprueba norma técnica para el desarrollo de sitios web de los órganos de la Administración del Estado.

17) D.S. N° 158 del 2007, del Ministerio Secretaria General de la Presidencia que Modifica D.S. N° 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
18) D.S. N° 475 de 1998, del Ministerio de Hacienda, Reglamento Ley 19.553 para la aplicación del incremento para el desempeño institucional del artículo 6° de la Ley y sus modificaciones.
19) Instructivo Presidencial N° 5 / 2001, Desarrollo de Gobierno Electrónico.
20) Instructivo Presidencial N° 04 del 2003, sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
21) Instructivo Presidencial N°6 del 2004, que imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la Administración Central del Estado.
22) Instrucción General N°2 del 2009, del Consejo de Transparencia, sobre la designación de enlaces con el Consejo para la Transparencia.
23) Instrucción General N° 3 del 2009, del Consejo para la Transparencia, que contiene el índice de actos o documentos calificados como secretes o reservados.
24) Documentos elaborados por el Comité de Normas para el Documento Electrónico.
25) 1nstructivo Presidencial N° 8 del 2006 sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
26) Circular N°3 del 2007, de Interior y Hacienda que detalla las medidas específicas que deben adoptar los Servicios y disponen los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.
27) Guía Metodológica del Sistema de Seguridad de la información, año 2012, de DIPRES.