APRUEBA LA "POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN", INSERTA EN EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE PREVISIÓN SOCIAL, APROBADA POR RESOLUCIÓN EXENTA N° 657, DE 2015.

RESOLUCIÓN EXENTA Nº 341

SANTIAGO, 13 JUL 2016

V I S T O S:

1.- La Ley N° 20.255, de Reforma Previsional, que establece la nueva Institucionalidad Pública para el Sistema de Previsión Social y crea entre sus órganos, el Instituto de Previsión Social determinando sus funciones y atribuciones; y el D.F.L. N° 4, de 2009, del Ministerio del Trabajo y Previsión Social que fija la Planta de Personal y fecha de iniciación de actividades de este Instituto.

2.- El D.F.L.N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado, de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

3.- La Ley N° 19.880, de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

4.- El D.S. N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confiabilidad de los Documentos Electrónicos; y el Decreto N° 100, de 2006, de la misma cartera ministerial, que aprueba la norma técnica para el desarrollo de Sitios Web de los Órganos de la Administración del Estado.

5.- La Ley N° 19.799, sobre firma y documentos electrónicos y su Reglamento contenido en el D.S. N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción.

6.- El D.F.L. N° 278, de 1960, del Ministerio de Hacienda; el D.L. N° 49, de 1973; el D.F.L. N° 17, de 1989, del Ministerio del Trabajo y Previsión Social; la Resolución N° 1600, de 2008, de la Contraloría General de la República, que fijó las normas sobre exención del trámite de toma de razón; y las facultades que me concede el artículo 57°, de la Ley N° 20.255.

CONSIDERANDO:

1.- Que, por Resolución Exenta N° 591, de 28 de diciembre de 2009, de la Dirección Nacional de este Instituto de Previsión Social, se aprobaron los documentos asociados a la "Política de Seguridad de la Información del IPS" y "Política de Gestión de Incidentes de Seguridad de la Información", instrumento modificado por la Resolución Exenta N° 83, de 10 de febrero de 2011, para los efectos de incorporar los textos de la "Política de Desarrollo y Mantenimiento de Sistemas" y "Política de Gestión de Continuidad de Negocio", todos los cuales resultan aplicables a todos los procesos de Seguridad del Instituto de Previsión Social y que respectivamente, forman parte integrante de dichos actos administrativos.

2.- Que, a través de Resolución Exenta N° 523, de 29 de octubre de 2012, se dispone una nueva constitución del Comité de Seguridad del Instituto de Previsión Social, integrado en forma permanente por los funcionarios que desempeñan los cargos de Subdirectores, Jefes de las Divisiones Jurídica, Informática, Planificación y Desarrollo, Beneficios y por el Encargado de Seguridad de la Información, dejando establecido la participación como invitado del Director Nacional, Jefe División Contraloría Interna, Jefe del Departamento de Personas y el Jefe del Departamento Compromisos Institucionales.

3.- Que, mediante Resolución Exenta N°170, de 10 de abril de 2015, se designa a la encargada de Seguridad del Instituto de Previsión Social, con dependencia de la Subdirección de Sistemas de la Información y de Administración de este Instituto, correspondiéndole actuar como asesora de esta Dirección Nacional para velar por preservar la confidencialidad, integridad y disponibilidad de la información, de conformidad con las normas legales y reglamentarias sobre la materia.

4.- Que, por Resolución Exenta N° 657, de 03 de diciembre de 2015, esta Dirección Nacional aprueba para este Instituto la "Política General de Seguridad de la Información" y en su Resuelvo N° 2, deja sin efecto el Resuelvo N°1 y el Resuelvo N°2, punto N°1, "Documento Política General de Seguridad de la Información" y "Documento Preliminar sobre Política de Seguridad, de la Resolución Exenta N°591, de 28 de diciembre de 2009, singularizada en el Considerando N° 1, del presente instrumento.

5.- Que, en el contexto indicado, la Encargada de Seguridad de la Información, ha propuesto el texto denominado "Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información", con la finalidad de asegurar una adecuada protección en el diseño, desarrollo, mantención y adquisición de los programas y aplicativos del IPS.

6.- Que, asimismo por Oficio Ordinario N°45126/2299-2016, de 23 de mayo de 2016, modificado por Oficio Ordinario N°45126/2725-2016, de 21 de junio del mismo año, la División Jurídica de este Instituto, aprueba y visa en cada una de sus páginas el proyecto denominado **"Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información"**, aprobado por el Comité de Seguridad de la Información, en sesión de fecha 04 de mayo de 2016, según consta en Acta de Reunión enviada por la Encargada de Seguridad de la Información, a través documento electrónico de 24 de junio de 2016, estableciendo la procedencia de emitir la Resolución aprobatoria de rigor, la que de conformidad a la Resolución N°1.600, de 2008, de la Contraloría General de la República, que fijó normas sobre exención del trámite de Toma de Razón, se encuentra exenta del mencionado trámite.

Departamento de Transparencia y Documentación – Instituto de Previsión Social
Avenida del Lib. Bernardo O'Higgins Nº 1353 – Santiago
[redacted] www.ips.gob.cl

R E S U E L V O:

1.- Apruébase, para el Instituto de Previsión Social la **"Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información"**, que consta de once (11) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 21 de junio de 2016, cuyo objetivo es asegurar una adecuada protección en el diseño, desarrollo, mantención y adquisición de los programas y aplicativos del IPS que se utilizan para apoyar las funciones criticas del negocio y garantizar que la seguridad sea parte integrante de los sistemas de información, y de los archivos involucrados a esos sistemas, prevenir errores, pérdida, modificaciones no autorizadas o mala utilización de la información de las aplicaciones del IPS.

2.- Cúmplase con lo dispuesto en el artículo 48°, de la Ley N°19.880, citada en Vistos N°3 Y en el Instructivo Presidencial Gab. Pres. N°008, de 04 de diciembre de 2006, complementado por Circular Conjunta N°3, de 05 de enero de 2007, del Ministerio del Interior y Ministerio de Hacienda, en orden a publicar el extracto del presente acto administrativo en el Diario Oficial y texto completo del mismo en el Banner "Gobierno Transparente".

3.- Publíquese el Procedimiento, que se aprueba por el presente acto administrativo, en el ambiente "Instructivos Institucionales", de la Intranet del IPS.

Notifíquese, regístrese y distribúyase por Departamento de Transparencia y Documentación, a las Jefaturas de las unidades incluidas en la Distribución de la presente Resolución.

INSTITUTO DE PREVISION SOCIAL
DIRECTOR NACIONAL

PATRICIO CORONADO ROJO
DIRECTOR NACIONAL
INSTITUTO DE PREVISIÓN SOCIAL

DISTRIBUCION:
- Gabinete Dirección Nacional
- Subdirección de Servicios al Cliente
- Subdirección de Sistema de Información y de Administración
- División Jurídica
- División Contraloría Interna
- División Beneficios
- División Canales de Atención a Clientes
- División Informática
- División Planificación y Desarrollo
- Departamento Auditoría Interna
- Departamento Comunicaciones
- Departamento de Transparencia y Documentación
- Departamento de Finanzas
- Departamento Administración e Inmobiliaria
- Departamento de Personas
- Departamento Cobranza Institucional
- A los Directores Regionales IPS, que deberán comunicar el presente instrumento a los Centros de Atención Previsional Integral de su dependencia
- Unidad Apoyo Documental de la División Jurídica
- A la Encargada de Seguridad del IPS

MEES/AC/AYGF/VO/M/VEV/MCR/ MBA/A/RPV/MRC/mrc
Aprueba "Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información"
VI (Folio DTD-3575-67-21)

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

CODIGO: POL-07

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
10/02/2011	01			Versión original del documento en Resolución Exenta N° 83 del 10-02-2011
06/01/2016	02	Todas		Actualización según versión de la norma ISO 27001:2013

La presente versión substituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie.

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 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.

NOTA DE CONFIDENCIALIDAD

La información contenida en este documento es de propiedad del Instituto de Previsión Social (IPS) y debe ser tratada de acuerdo a su nivel de confidencialidad, sobre la base de las instrucciones establecidas en la política de clasificación y manejo de información. 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 al Instituto de Previsión Social.

ÍNDICE

1. OBJETIVO

Asegurar una adecuada protección en el diseño, desarrollo, mantención y adquisición de los programas y aplicativos del IPS que se utilizan para apoyar las funciones críticas del negocio y garantizar que la seguridad sea parte integral de los sistemas de información, y de los archivos involucrados a esos sistemas, prevenir errores, pérdida, modificaciones no autorizadas o mala utilización de la información de las aplicaciones de IPS.

2. ALCANCE

Se aplica a todo desarrollo, mantenimiento, adquisición de aplicaciones y activos de información, dentro del alcance definido para el sistema de seguridad de la información, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger los activos de información que se encuentren en otras formas.

Cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

3. DOCUMENTOS DE REFERENCIA

CONTROL LEGAL Y NORMATIVO.

República de Chile
• La Constitución Política de la República de Chile. • Código Penal de la República de Chile. • Circular N° 3, enero de 2007, de los Ministerios del Interior y de Hacienda: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado • Decreto Supremo N° 83/2004, 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. • Decreto Supremo N° 93/2006 del Ministerio Secretaria General de la Presidencia, Norma Técnica para la Adopción de Medidas destinadas a Minimizar los efectos Perjudiciales de los Mensajes Electrónicos Masivos no solicitados.

República de Chile

- Decreto 779, noviembre 2000, reglamento del registro de bancos de datos personales a cargo de organismos públicos.
- Decreto 277. Reglamento de Propiedad Intelectual.
- Instructivo Presidencial N° 05, mayo de 2001: Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.
- Instructivo Presidencial N° 06, junio de 2004: Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.
- Instrucción General N°2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
- Instrucción General N°3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados.
- Instructivo Presidencial N°08, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
- Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
- Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido fue fijado por el D.F.L. N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia.
- Ley N° 18.834, cuyo texto refundido fue fijado por el D.F.L N° 29, de 2004, del Ministerio de Hacienda.
- La Ley N° 19.880, que establece las "Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado".
- Ley Nº 20.285 sobre "Transparencia y Acceso a la Información Pública", y su Reglamento contenido en el Decreto Nº 13, de 2009, del Ministerio Secretaría General de la Presidencia.
- Ley N° 19.628, agosto de 1999, sobre "Protección de la Vida Privada y Datos Personales", Ministerio Secretaria General de la Presidencia.
- Ley Nº 17.336, octubre de 1970, sobre "Propiedad Intelectual", Ministerio de Educación.
- Ley Nº 19.223, junio de 1993, sobre "Delitos informáticos" del Ministerio de Justicia.
- Ley N°19.799, abril de 2002. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.
- Ley 18.168, Ley General de Telecomunicaciones.
- Ley 19.927, Modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en Materia de Delitos de Pornografía Infantil.
- Ord., Nº 1902-229 del 23/12/2011, del Director Nacional, que imparte instrucciones

República de Chile
programáticas en materia de Gestión de Seguridad de la Información con el objeto que las jefaturas tomen medidas pertinentes en relación al personal de su dependencia o que se desempeñe en sus unidades dependientes. • Resolución Exenta N° 170, de 10 de abril de 2015, que designó al Encargado de Seguridad de la Información. • OS N°181/2002 del Ministerio de Economía, Fomento y Reconstrucción Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
NCh-ISO 27001:2013
14.1.1 Análisis y especificación de requisitos de seguridad de la información. 14.1.2 Aseguramiento de servicios de aplicación en redes públicas. 14.1.3 Protección de las transacciones de servicios de aplicación. 14.2.1 Política de desarrollo seguro. 14.2.2 Procedimientos de control de cambios de sistemas. 14.2.6 Entorno de desarrollo seguro. 14.2.7 Desarrollo tercerizado. 14.2.9 Prueba de aprobación del sistema. 14.3.1 Protección de datos de prueba.

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Política General de Seguridad de la Información	Política General de Seguridad de la Información.pdf

4. DEFINICIONES

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).

Custodio de la información: Funcionario que mantiene bajo su responsabilidad información de la que no es propietario, pero por su función es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos.

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

Información Pública: Es aquella información cuyo conocimiento no está circunscrito, se presume pública toda la información que obre en poder de la Administración del Estado, salvo en los casos de excepción contemplados en el artículo 21 de la Ley N°20.285.

Información Interna: Es aquella información cuyo conocimiento está circunscrito a los todos los funcionarios de la organización.

Negocio: Función o servicio prestado por 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: Probabilidad de ocurrencia de un evento inesperado.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudio y confiabilidad.

Tercero: Empresa externa que brinda un servicio a IPS.

IPS: Instituto de Previsión Social.

5. RESPONSABILIDADES

Comité de Seguridad de la Información (CSI): Es responsable ante la Dirección Nacional por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades de IPS, los recursos disponibles y la normativa vigente.

Encargado de Seguridad de la Información (ESI): Es el representante del Director Nacional en la definición y aplicación de los criterios de seguridad de la información en IPS. Responsable de velar por el cumplimiento de las políticas de seguridad de la información, sus normas y procedimientos. Asesora al Director Nacional en materia de Seguridad de la Información, y dirige el Comité de Seguridad de la Información.

División Informática: Debe velar por el cumplimiento de los procedimientos definido en esta política respecto a un desarrollo seguro y una adquisición y mantenimiento responsable.

Funcionario del IPS: 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 por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

Jefe del Departamento de Seguridad de Información: Encargado de velar por las políticas y procesos relativos a la seguridad de la información en IPS. Responsable técnico de implementar las medidas de seguridad en la institución para la protección de la red, datos y sistemas. Responsable de actualizar esta política.

Jefe del Departamento de Desarrollo y Mantención: Es responsable implementar ésta política e informar al Jefe de la División Informática, cada vez que sea transgredida.

Jefe de la División Jurídica: Encargada de instruir los procesos disciplinarios que correspondan, ante hechos que pueden revestir el carácter de delitos y/o conductas sancionables en materia administrativa.

Jefe del Departamento de Administración e Inmobiliaria: Encargado de cumplir los procesos definidos por IPS para la adquisición de sistemas de información.

6. POLÍTICA

6.1. Requisitos de seguridad de los sistemas de información.

6.1.1. Se debe informar al personal interno o externo de sus obligaciones y responsabilidades técnicas.

6.1.2. En el caso que los productos son adquiridos, se debe seguir un proceso formal de pruebas previo a la aceptación de los mismos.

6.1.3. Los contratos con el proveedor deben ser respaldados con un acuerdo de confidencialidad y documentos que comprometan a ambas partes para cumplir los términos de servicios acordados.

6.1.4. IPS puede contratar los servicios de certificación de firma electrónica con entidades certificadoras acreditadas y/o convenio Segpres, si resulta conveniente técnica o económicamente.

6.1.5. El responsable del negocio, en conjunto con el Jefe de Departamento de Seguridad de Información, deben evaluar la necesidad de usar tecnologías de encriptación para proteger información, o de tecnologías de firma digital para firmar documentos electrónicos.

6.1.6. La información implicada en transacciones de servicio se debe proteger para evitar la transmisión incompleta, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.

6.1.7. Los cambios en los sistemas deben ser controlados por un procedimiento formal, de control de cambios.

6.2. Seguridad en los procesos de desarrollo y soporte

6.2.1. Debe utilizarse un sistema de versionado para mantener el control del software implementado, archivos de configuración, así como la documentación de sistema. Se deben establecer estándares para la metodología de desarrollo, los lenguajes de programación, que pueden ser diversos.

6.2.2. Se debe contar con un procedimiento para el registro y control de los cambios realizados. Asimismo, se debe tener la aprobación formal del negocio de los cambios del software realizados antes de la implementación. Todo desarrollo o mantenimiento, se debe guiar por las políticas y procedimientos de la organización en esta materia.

6.2.3. La notificación de cambios al software de base debe ser realizada con suficiente antelación para permitir realizar pruebas y revisiones apropiadas antes de la puesta en producción.

6.2.4. Se debe conservar el software original y los cambios deben ser aplicados a una copia claramente identificada. Se debe prevenir pérdida de datos, de usuarios, en las aplicaciones de los sistemas, utilizando controles y seguimientos de auditorías o registros de actividad.

6.2.5. Debe existir una estrategia de "vuelta atrás" antes de que los cambios sean implementados. Todos los cambios de sistema deben ser probados y documentados, de modo que ellos puedan ser vueltos a aplicar si fuera necesario a futuras mejoras de software.

6.2.6. Se debe evaluar la información expuesta en internet y los desarrollos que se encuentran en producción, con el fin de verificar la existencia de fuga de información sensible.

6.2.7. El desarrollo externo de software debe ser supervisado y/o monitoreado por un funcionario designado por IPS.

6.2.8. Deben separarse las bibliotecas de fuentes de Desarrollo, QA y Producción. Se debe mantener un nivel de seguridad para que el software en Producción no se vea afectado por el desarrollo o mantención de sistemas.

6.2.9. Se deben llevar a cabo pruebas antes de la instalación para detectar posibles vulnerabilidades de seguridad.

6.2.10. Se deben cambiar las claves por defecto en los sistemas comprados a terceros, antes de ser puestos en producción.

6.3. Protección de los datos utilizados en pruebas.

6.3.1. Debe asegurarse que los entornos de producción y sus bibliotecas sean actualizados de forma coordinada con los entornos de prueba.

7. DIFUSIÓN

La política de adquisición, desarrollo y mantenimiento de los sistemas de información, sus normas, procedimientos y sus correspondientes actualizaciones y/o modificaciones, como también las resoluciones, oficios y/o circulares que emanen de la Dirección Nacional o del Encargado de Seguridad de la Información, deben ser publicados en la página de la intranet del IPS.

El Encargado de Seguridad de la Información en conjunto con el Departamento de Seguridad de la Información, impulsarán un Plan de Comunicación o Sensibilización de las políticas organizacionales de la Seguridad de la Información, además de otras acciones de comunicación y difusión por los distintos medios que posee la institución.

8. REEVALUACIÓN

Esta política de adquisición, desarrollo y mantenimiento de los sistemas de información y sus normas, que se aplican a los activos de información serán examinados, revisados y reevaluados por el Comité de Seguridad de la Información, cada tres (3) años y extraordinariamente cuando ocurra un incidente de seguridad o cambio normativo que afecte a un activo de información catalogado con riesgo medio y/o alto, de manera de introducir las modificaciones apropiadas.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.